MATHEMATISCHE ZEITSCHRIFT

UNTER STÄNDIGER MITWIRKUNG
VON

K. KNOPP
KÖNIGSBERG

E. SCHMIDT
BERLIN

I. SCHUR
BERLIN

HERAUSGEGEBEN
VON

L. LICHTENSTEIN
LEIPZIG

WISSENSCHAFTLICHER BEIRAT:

W. BLASCHKE L. FEJÉR E. HECKE G. HERGLOTZ A. KNESER
E. LANDAU O. PERRON F. SCHUR E. STUDY H. WEYL

19. BAND 3./4. HEFT

(AUSGEGEBEN AM 31. JANUAR 1924)

BERLIN
VERLAG VON JULIUS SPRINGER
1924

Die

MATHEMATISCHE ZEITSCHRIFT

erscheint in zwanglosen Heften, deren vier zu einem Bande vereinigt werden sollen.

Jährlich sollen drei Bände herausgegeben werden. Die Mathematische Zeitschrift ist durch jede Buchhandlung sowie durch die Verlagsbuchhandlung zu beziehen.

Die Mathematische Zeitschrift dient der Pflege der reinen Mathematik, doch werden natürlich auch Beiträge aus den Gebieten der theoretischen Physik und Astronomie Aufnahme finden, soweit sie mathematisch von Interesse sind. Besprechungen, Aufgaben u. dgl. werden nicht zugelassen.

Die Verfasser erhalten von Abhandlungen bis zu 24 Seiten Umfang 100 Sonderabdrucke, von größeren Arbeiten 50 Sonderabdrucke kostenfrei, weitere gegen Berechnung.

Manuskriptsendungen sind zu richten an die Mitglieder der unterzeichneten Schriftleitung. Die Herren Mitarbeiter werden im Interesse einer raschen Drucklegung gebeten, die Arbeiten in gut lesbarer Niederschrift, etwaige Abbildungen auf einem besonderen Blatt gezeichnet, einzureichen. Die in den Formeln etwa vorkommenden griechischen oder deutschen Buchstaben (Fraktur) sind stets besonders (etwa mit einem farbigen Stift) zu kennzeichnen. Der Text ist in lateinischer Schrift abzufassen. Die Fußnoten sind fortlaufend zu numerieren, bei Zitaten Erscheinungsjahr und Seitenzahlen anzugeben.

SCHRIFTLEITUNG DER MATHEMATISCHEN ZEITSCHRIFT:

K. Knopp, Königsberg, Bergplatz 6,
L. Lichtenstein, Leipzig, Talstraße 35, Mathematisches Institut,
E. Schmidt, Berlin NW, Altonaerstr. 30,
I. Schur, Berlin-Schmargendorf, Ruhlaerstr. 14.

---

19. Band. **Inhalt:** 3./4. Heft.

Seite

Artin, E., Quadratische Körper im Gebiete der höheren Kongruenzen. I. (Arithmetischer Teil.) 153

Artin, E., Quadratische Körper im Gebiete der höheren Kongruenzen. II. (Analytischer Teil.) 207

Kamke, E., Zur Arithmetik der Polynome 247

Weinstein, A., Ein hydrodynamischer Unitätssatz 265

Ore, Ö., Algebraische Gleichungen mit primitiven Gruppen 276

Haupt, O., Über Kurven endlicher Ordnung 284

Walfisz, A., Über Gitterpunkte in mehrdimensionalen Ellipsoiden 300

Bauer, M., Über die Erweiterung des Körpers der p-adischen Zahlen zu einem algebraisch abgeschlossenen Körper 308

Quadratische Körper im Gebiete der höheren Kongruenzen. I.

(Arithmetischer Teil.)

Von

E. Artin in Hamburg.

§ 1.

Einleitung.

Die Dedekindschen Untersuchungen über höhere Kongruenzen[1]) legen folgende Erweiterung der Theorie nahe.

Es werde dem Körper K der rationalen Funktionen modulo p die Funktion $\sqrt{D(t)}$ adjungiert, wo $D(t)$ eine ganze im Sinne Dedekinds quadratfreie Funktion des Parameters t ist. Der entstehende quadratische Körper $K(\sqrt{D(t)})$ weist dann ähnliche Eigenschaften auf wie ein quadratischer Zahlkörper.

So gilt zum Beispiel der Satz über eindeutige Zerlegbarkeit der Ideale in Primideale, der Satz von der Endlichkeit der Klassenzahl, die Sätze über die Einheiten.

Zur Klassenzahlformel gelangt man durch Einführung der Zetafunktionen. Hier läßt sich die Frage nach der Richtigkeit der Riemannschen Vermutung in jedem speziellen Fall entscheiden. Eine Durchrechnung der ersten Fälle — es handelt sich um zirka vierzig Körper — ergab stets die Richtigkeit der Riemannschen Vermutung. Einem allgemeinen Beweis ihrer Richtigkeit scheinen sich aber noch Schwierigkeiten ähnlicher Art wie beim Riemannschen $\zeta(s)$ entgegenzustellen, doch liegen die Verhältnisse hier insofern klarer und durchsichtiger, als es sich (im wesentlichen) um ganze rationale Funktionen handelt. Auf Fragen, die damit im Zusammenhang stehen, werde ich noch zurückkommen.

Von den sonstigen Eigenschaften unserer Zetafunktionen sei noch hervorgehoben: Sie besitzen eine einfache Funktionalgleichung, welche als

[1]) Journ. für die r. u. a. Math. **54** (1857), S. 1–26.

Folge merkwürdige Reziprozitätsbeziehungen gewisser Charaktersummen nach sich zieht. Ihre Nullstellen stehen in einfachem Zusammenhang mit den Wurzeln einer algebraischen Gleichung, wodurch eben die Entscheidung über die Riemannsche Vermutung gefällt werden kann.

Setzt man die Richtigkeit der Riemannschen Vermutung für alle Körper voraus, so läßt sich für alle p der Nachweis erbringen, daß es nur endlich viele imaginäre Körper mit einklassigen Geschlechtern gibt.

Endlich sei auch noch auf den Zusammenhang mit einer Arbeit von Kornblum[2]), der am Schlusse des zweiten Teils dieser Arbeit hergestellt wird, hingewiesen. Es gelingt dabei, das Kornblumsche Resultat über die Existenz unendlich vieler Primfunktionen in arithmetischen Progressionen wesentlich zu verschärfen.

Bemerkt sei noch, daß ich der kürzeren Bezeichnung halber einige im Gebiete der Zahlen verwendete Symbole sinngemäß auf die Funktionen (mod p) übertragen habe. Dies rechtfertigt sich auch schon dadurch, daß dann die Analogie unserer Resultate mit denen in Zahlkörpern deutlicher zutage tritt. Eine Verwechslung ist dabei wohl nicht zu befürchten, da die Symbole nur gemäß unserer Definition verwendet werden.

§ 2.

Erste Erweiterung des Rechengebietes.

Nach Dedekind heißen zwei Funktionen $F_1(t) = \sum_{\nu=0}^{n} a_\nu t^\nu$ und $F_2(t) = \sum_{\nu=0}^{n} b_\nu t^\nu$ kongruent modulo p, in Zeichen

$$F_1(t) \equiv F_2(t) \pmod{p},$$

wenn für alle ν gilt

$$a_\nu \equiv b_\nu \pmod{p}.$$

Dabei bedeutet p eine in den ganzen Entwicklungen festgehaltene Primzahl.

Wir wollen in diesem Falle die Funktionen und Zahlen direkt „gleich“ nennen und also einfach schreiben

$$F_1(t) = F_2(t), \quad \text{wenn} \quad a_\nu = b_\nu.$$

Von Vielfachen von p ist hierbei eben abgesehen.

Ferner verstehen wir, wenn $a \not\equiv 0 \pmod{p}$ (d. h. nach der vorigen Festsetzung $a \not\equiv 0 \pmod{p}$), unter $\frac{b}{a}$ eine Zahl x, für welche $ax = b$ ist (d. h. wieder $ax \equiv b \pmod{p}$). Zum Beispiel ist, wenn p ungerade, unter der häufig auftretenden Zahl $\frac{1}{2}$ die ganze Zahl $\frac{p+1}{2}$ zu verstehen.

---

[2]) Mathem. Zeitschr. 5 (1919), S. 100.

Nun lassen wir — und darin besteht unsere Erweiterung — auch negative Potenzen von t in endlicher oder unendlicher Anzahl zu. Wir betrachten also Funktionen der Form

$$F(t) = \sum_{\nu=-\infty}^{n} a_\nu t^\nu = a_n t^n + a_{n-1} t^{n-1} + \ldots \qquad (n \gtrless 0),$$

wobei wieder zwei Funktionen „gleich" sein sollen, wenn die Koeffizienten entsprechender t-Potenzen „gleich" sind.

Man beachte, daß dem Buchstaben t keinerlei numerische Bedeutung zukommt, und er lediglich als Rechensymbol zu betrachten ist, so daß im Falle unendlich vieler negativer Potenzen von t der Konvergenzfrage keinerlei Bedeutung zukommt. Da er ferner im allgemeinen derselbe bleibt, unterdrücken wir künftighin seine Bezeichnung, schreiben also kurz

$$F \quad \text{statt} \quad F(t).$$

Zahlen mögen stets mit kleinen lateinischen Buchstaben und den allgemein üblichen Summationsbuchstaben μ, ν bezeichnet werden, alle übrigen Buchstaben seien den Funktionen vorbehalten.

Sei nun $F = \sum_{\nu=-\infty}^{n} a_\nu t^\nu$, wobei $a_n \neq 0$ vorausgesetzt sei.

F heiße ganz, wenn die Koeffizienten aller negativen Potenzen von t verschwinden, wenn es also eine Funktion im Dedekindschen Sinne ist.

Ferner heiße für ganzes und nicht ganzes F:

1. Wie bei Dedekind, n der Grad von F.

2. Die Zahl p^n der „Betrag" $|F| = p^n$ von F. Diese Bezeichnung wird sich in der Folge rechtfertigen. Für jetzt sei nur bemerkt, daß im Falle eines ganzen F die Zahl $p^n = |F|$ die Anzahl der Restklassen der ganzen Funktionen modulo F ist. In der Dedekindschen Bezeichnung (modd $p, F(t)$). Für von Null verschiedene Zahlen a gilt dann $|a| = 1$. Ferner werde $|0| = 0$ gesetzt.

3. Der Koeffizient a_n der höchsten Potenz von t, der schon bei Dedekind die Rolle des „Vorzeichens" von F spielt, werde mit

$$a_n = \operatorname{sgn} F$$

bezeichnet. Diese Definition hat natürlich nur einen Sinn, wenn $F \neq 0$ ist, d. h. wenn es nichtverschwindende Koeffizienten überhaupt gibt. Dann ist $\operatorname{sgn} F \neq 0$.

4. Mit Dedekind nennen wir die von Null verschiedenen Zahlen $1, 2, \ldots, (p-1)$ die rationalen Einheiten, da sie in *unserem* Sinne *Teiler* der Eins sind.

5. Wenn $\operatorname{sgn} F = 1$ ist, heiße F primär. (Es entspricht dies ungefähr den positiven Zahlen.)

Für unsere Symbole gelten nun ersichtlich die gewöhnlichen Rechenregeln:

$$|FG| = |F| \cdot |G|,$$

$\operatorname{sgn}(FG) = \operatorname{sgn} F \cdot \operatorname{sgn} G$.

Wir erwähnen noch die folgenden häufig zur Verwendung gelangenden Regeln:

1. Wenn $|F| < |G|$, so ist

$$|F + G| = |G|.$$

Hier hat ja F auf den Grad des Resultats keinen Einfluß. Ebenso gilt unter der gleichen Voraussetzung

$$\operatorname{sgn}(F + G) = \operatorname{sgn} G.$$

2. Wenn $|F| = |G|$ und $\operatorname{sgn} F + \operatorname{sgn} G \neq 0$ ist, gilt

$$|F + G| = |F| = |G|$$

und

$$\operatorname{sgn}(F + G) = \operatorname{sgn} F + \operatorname{sgn} G.$$

3. Wenn $|F| = |G|$ und $\operatorname{sgn} F + \operatorname{sgn} G = 0$ ist, haben wir

$$|F + G| < |F| = |G|.$$

Der Beweis dieser Sätze folgt unmittelbar aus Gradbetrachtungen.

Das Rechnen mit Grenzwerten erhalten wir durch folgende *Definition*:

Eine Folge von Funktionen $F_1, F_2, F_3, \ldots$ konvergiert gegen einen Grenzwert, in Zeichen $F = \lim_{\nu=\infty} F_\nu$, wenn sich nach Vorgabe eines beliebig kleinen positiven ε ein n so finden läßt, daß für alle $\nu \geqq n$ gilt

$$|F_\nu - F| \leqq \varepsilon.$$

Das heißt ein beliebig gegebener Abschnitt von F kommt von einer Stelle n ab in allen F_ν vor.

Ersichtlich ist hierfür notwendig und hinreichend, wenn eine Stelle n existiert, so daß für $\mu, \nu \geqq n$ gilt

$$|F_\nu - F_\mu| \leqq \varepsilon.$$

Aus dem Grenzwertbegriff folgt unmittelbar der Begriff der Konvergenz und der Summe einer unendlichen Reihe

$$\sum_{\nu=0}^{\infty} F_\nu.$$

Sie konvergiert und hat die Summe S, wenn $S = \lim_{n=\infty} S_n$ existiert, wo

$$S_n = \sum_{\nu=0}^{n} F_\nu.$$

Für die Konvergenz ist notwendig und hinreichend, daß für alle genügend großen μ und $\nu \geqq \mu$ die Beträge der Ausschnitte $F_\mu + F_{\mu+1} + \ldots + F_\nu$ beliebig klein werden.

Da nun einerseits die Beträge dieser Ausschnitte nach unseren Rechenregeln die der einzelnen Glieder nie überschreiten können und andererseits als Ausschnitte für $\mu = \nu$ die einzelnen Glieder selbst auftreten, erhalten wir das einfache Konvergenzkriterium:

Für die Konvergenz der unendlichen Reihe (1) ist notwendig und hinreichend, daß

$$\lim_{\nu=\infty} |F_\nu| = 0.$$

Insbesondere erhalten wir für „Potenzreihen“

$$\sum_{\nu=0}^{\infty} a_\nu F^\nu,$$

deren Koeffizienten Zahlen sind, daß sie sicher konvergieren für

$$|F| \leqq p^{-1}.$$

Denn dann ist:

$$|a_\nu F^\nu| \leqq p^{-\nu}, \quad \text{also} \quad \lim_{\nu=\infty} |a_\nu F^\nu| = 0.$$

Ebenso leicht erhalten wir die Resultate:

Jede konvergente Reihe konvergiert unbedingt, d. h. ihre Glieder können beliebig vertauscht werden.

Für das Produkt zweier konvergenter Reihen gilt die Cauchysche Produktregel.

Definition. Wenn $G \neq 0$ ist, verstehen wir unter $H = \frac{F}{G}$ eine Funktion, für welche $HG = F$ ist.

Um die Existenz einer solchen Funktion nachzuweisen, sei

$$G = a_n t^n + a_{n-1} t^{n-1} + \ldots = a_n t^n (1 - \Phi),$$

wobei $a_n \neq 0$ vorausgesetzt wird. Hier ist

$$\Phi = -\frac{a_{n-1}}{a_n} t^{-1} - \frac{a_{n-2}}{a_n} t^{-2} - \ldots, \quad \text{also} \quad |\Phi| \leqq p^{-1}.$$

Demnach konvergiert

$$\sum_{\nu=0}^{\infty} \Phi^\nu,$$

und es ist

$$(1 - \Phi) \sum_{\nu=0}^{\infty} \Phi^\nu = \sum_{\nu=0}^{\infty} \Phi^\nu - \sum_{\nu=1}^{\infty} \Phi^\nu = 1.$$

Setzen wir also

$$H = a_n^{-1} t^{-n} \cdot F \cdot \sum_{\nu=0}^{\infty} \Phi^\nu,$$

so gilt $HG = F$. Also ist H eine Funktion der gesuchten Art. Aus $AB = 0$ und $A \neq 0$ folgt aber durch Betrachtung der Beträge $B = 0$.

Wäre also H_1 eine zweite Funktion, für die $H_1 G = F$ ist, so wäre $(H - H_1) G = 0$. Wegen $G \neq 0$ folgt $H = H_1$. Also ist $H = \frac{F}{G}$ eindeutig bestimmt.

Aus

$$|F| = |HG| = |H| \cdot |G|$$

folgt die Rechenregel

$$\left|\frac{F}{G}\right| = \frac{|F|}{|G|}$$

und analog ist

$$\operatorname{sgn} \frac{F}{G} = \frac{\operatorname{sgn} F}{\operatorname{sgn} G}.$$

Endlich definieren wir:

Definition. Alle Funktionen, die sich als Quotient zweier ganzer Funktionen darstellen lassen, heißen rational, alle übrigen irrational.

§ 3.

Quadratische Gleichungen und Imaginäre.

Für das Weitere beschränken wir uns auf ungerade Primzahlmoduln p. Wir untersuchen nun die quadratische Gleichung

$$X^2 = A.$$

Wir erkennen leicht, daß diese Gleichung keine unserem bisherigen Rechengebiete angehörige Lösung haben kann, wenn

1. A ungeraden Grad hat, oder
2. $\operatorname{sgn} A$ quadratischer Nichtrest modulo p ist.

Wenn dagegen A von geradem Grade und $\operatorname{sgn} A = a^2$ ein quadratischer Rest ist, hat unsere Gleichung stets genau zwei nur durch das Vorzeichen verschiedene Lösungen. Denn dann hat A die Form

$$A = a^2 t^{2n} + a_{2n-1} t^{2n-1} + \ldots = a^2 t^{2n} (1 + \Phi),$$

wobei

$$\Phi = \frac{a_{2n-1}}{a^2} t^{-1} + \frac{a_{2n-2}}{a^2} t^{-2} + \ldots, \quad \text{also} \quad |\Phi| \leqq p^{-1}.$$

Nun ist

$$\binom{\frac{1}{2}}{\nu} = \frac{\frac{1}{2} \cdot (-\frac{1}{2}) \ldots (\frac{1}{2} - \nu + 1)}{\nu!} = \frac{(-1)^{\nu-1}}{2^\nu} \frac{1 \cdot 3 \cdot 5 \ldots (2\nu - 3)}{\nu!}$$

oder

$$\binom{\frac{1}{2}}{\nu} = \frac{(-1)^{\nu-1}}{2^{2\nu-1}(\nu-1)} \cdot \binom{2\nu-2}{\nu} = \frac{(-1)^{\nu-1}}{2^{2\nu-1}\nu} \cdot \binom{2\nu-2}{\nu-1}.$$

Aus der letzten Gleichheit geht, da $(\nu - 1)$ und ν zueinander prim sind, hervor, daß im Nenner von $\binom{\frac{1}{2}}{\nu}$ nur Potenzen von 2 auftreten können. Da wir die Primzahl p als ungerade voraussetzen (der Grund dafür ist das soeben festgestellte Verhalten), können wir $\frac{1}{2}$ durch die ganze Zahl $\frac{p+1}{2}$ ersetzen. Die so entstehende ganze Zahl $\binom{\frac{1}{2}}{\nu}$ gehorcht dann denselben Gesetzen wie das gewöhnliche Symbol, falls nur die Gleichheitszeichen in unserem Sinne als Kongruenzen gelesen werden.

Demnach ist das Quadrat der nach dem Früheren wegen $|\Phi| \leqq p^{-1}$ konvergenten Potenzreihe

$$\sum_{\nu=0}^{\infty} \binom{\frac{1}{2}}{\nu} \Phi^{\nu}$$

(nach der Cauchyschen Regel berechnet) gleich $1+\Phi$, da dies im gewöhnlichen Zahlgebiet der Fall ist.

Die Funktion

$$X = at^n \sum_{\nu=0}^{\infty} \binom{\frac{1}{2}}{\nu} \Phi^{\nu}$$

ist also eine Lösung von $X^2 = \Delta$. Wäre noch $X_1^2 = \Delta$, so hätten wir $X^2 - X_1^2 = 0$ oder $(X + X_1)(X - X_1) = 0$, somit entweder $X = X_1$ oder $X = -X_1$.

Wir schreiben $\sqrt{\Delta} = X$, wo das Vorzeichen noch beliebig wählbar ist, und nennen $\sqrt{\Delta}$ in diesem Falle reell.

Um das Symbol $\sqrt{\Delta}$ auch in den ausgeschlossenen, „imaginären" Fällen zu definieren, gehen wir so vor:

Sei g eine primitive Kongruenzwurzel modulo p, die im weiteren Verlaufe festgehalten werde.

Wir führen nun die beiden „Imaginären" $\sqrt{g}$ und $\sqrt{t}$ ein und betrachten Funktionen der Art:

1. $A + B\sqrt{g}$,
2. $A + B\sqrt{t}$,
3. $A + B\sqrt{gt}$.

Unter Aufrechterhaltung der formalen Rechenregeln für Addition und Multiplikation setzen wir fest, daß $A + B\sqrt{t} = C + D\sqrt{t}$ dann und nur dann zutrifft, wenn $A = C$ und $B = D$ ist. Analog in den übrigen Fällen. Mit den drei Arten werde aber nicht simultan gerechnet. Man überzeugt sich leicht, daß die Aufrechterhaltung der Rechenregeln auf keinen Widerspruch führt, und daß aus dem Verschwinden eines Produktes

auf das Verschwinden eines der Faktoren geschlossen werden darf. In der Tat, wird die Imaginäre mit i bezeichnet, so folgt aus

$$(A+iB)(C+iD)=0 \quad \text{auch} \quad (A-iB)(C-iD)=0,$$

also

$$(A^2-i^2B^2)(C^2-i^2D^2)=0.$$

Ist nun $A+iB\neq 0$, das heißt verschwinden A und B nicht gleichzeitig, so sind für $i=\sqrt{t}$ oder $i=\sqrt{gt}$ die Grade von A^2 und i^2B^2 sicher verschieden (gerade und ungerade), für $i=\sqrt{g}$ sicher die „Signa". Also ist auch $A^2-i^2B^2\neq 0$. Somit $C^2-i^2D^2=0$. Nach dem eben Gezeigten geht dies nur, wenn $C=D=0$, also $C+iD=0$ ist.

Von der Möglichkeit und Eindeutigkeit der Division überzeugt man sich ebenfalls sofort durch „Rationalmachen" des Nenners.

Für die beiden ausgeschlossenen Fälle ergibt nun eine einfache Betrachtung folgende Möglichkeiten:

1. $\sqrt{\frac{\Delta}{g}}$ ist reell $=\sqrt{\Delta_1}$,
2. $\sqrt{\frac{\Delta}{t}}$ ist reell $=\sqrt{\Delta_1}$,
3. $\sqrt{\frac{\Delta}{gt}}$ ist reell $=\sqrt{\Delta_1}$.

Es ist hier der Ort darauf hinzuweisen, daß es oft zweckmäßig ist, den Parameter t einer linearen Transformation der Form $t_1=at+b$ zu unterwerfen. Durch diese wird offenbar keine zahlentheoretische Eigenschaft unserer Funktionen geändert und doch manche Vereinfachung erzielt. So läßt sich zum Beispiel durch $t_1=gt$ Fall 3 auf Fall 2 zurückführen, so daß es genügte, die Diskussionen für die ersten beiden Fälle durchzuführen. Wir werden gelegentlich von diesen Lineartransformationen Gebrauch zu machen haben.

Die Lösungen von $X^2=\Delta$ lassen sich also in vier Klassen teilen ($\sqrt{\Delta_1}$ bedeute eine reelle Wurzel):

1. $\sqrt{\Delta}$ reell,
2. $\sqrt{\Delta}=\sqrt{g}\cdot\sqrt{\Delta_1}$,
3. $\sqrt{\Delta}=\sqrt{t}\cdot\sqrt{\Delta_1}$,
4. $\sqrt{\Delta}=\sqrt{gt}\cdot\sqrt{\Delta_1}$,

wobei Fall 3 und 4 nicht wesentlich verschieden sind.

Für die Lösung der quadratischen Gleichung

$$AX^2+BX+C=0 \qquad (A\neq 0)$$

ergibt sich nun in bekannter Weise

$$X=\frac{-B\pm\sqrt{B^2-4AC}}{2A}=\frac{-B\pm\sqrt{\Delta}}{2A}.$$

§ 4.

Quadratische Körper.

In der zuletzt aufgestellten quadratischen Gleichung mögen nun A, B, C ganze Funktionen sein. Zerlegen wir $\Delta = B^2 - 4AC$ in seine Primfaktoren, so können wir Δ in die Form setzen

$$\Delta = M^2 \cdot D,$$

wo D quadratfrei ist und überdies entweder $\operatorname{sgn} D = 1$ oder $\operatorname{sgn} D = g$. (Indem nämlich ein quadratischer Rest zu M gezogen wird.)

Dann ist $\sqrt{\Delta} = M \cdot \sqrt{D}$. Man erkennt leicht, daß $\sqrt{D}$ nur im Falle $D = 1$, den wir weiterhin als trivial ausschließen, reell und rational ist.

Die Lösung unserer Gleichung hat dann die Form

$$X = \frac{-B \pm M\sqrt{D}}{2A}.$$

Funktionen dieser Form nennen wir quadratische Irrationalitäten und zwar reell oder imaginär, je nachdem $\sqrt{D}$ reell oder imaginär ist.

Die Gesamtheit aller rationalen Funktionen modulo p bildet nun offenbar einen Körper K.

Wir untersuchen nun den Körper Ω, der durch Adjunktion einer quadratischen Irrationalität zu K entsteht. Diese Adjunktion kann offenbar ersetzt werden durch Adjunktion von $\sqrt{D}$. Wir definieren also (Vorzeichen von $\sqrt{D}$ beliebig fest gewählt):

Ist $D \neq 1$ eine ganze quadratfreie Funktion $\bmod p$ und $\operatorname{sgn} D = 1$ oder g, so entsteht der „quadratische Körper“ $\Omega = K(\sqrt{D})$ durch Adjunktion von $\sqrt{D}$ zum Körper K. Der Körper heißt reell oder imaginär, je nachdem ob $\sqrt{D}$ reell oder imaginär ist.

Die Funktionen des Körpers $K(\sqrt{D})$ lassen sich darstellen in der Form

$$\alpha = A + B\sqrt{D},$$

wo A und B rational sind.

Sie lassen sich auch nur auf eine Weise so darstellen, denn aus $A + B\sqrt{D} = C + E\sqrt{D}$ würde im Falle $B \neq E$ folgen $\sqrt{D} = \frac{A-C}{E-B}$, so daß $\sqrt{D}$ reell rational wäre. Aus $B = E$ folgt aber wieder $A = C$.

α genügt der Gleichung

$$\alpha^2 - 2A\alpha + (A^2 - DB^2) = 0.$$

Die zweite Wurzel dieser Gleichung

$$\alpha' = A - B\sqrt{D}$$

heißt die zu α konjugierte Funktion. Endlich heißt $\alpha\alpha'$ die Norm von α:

$$N(\alpha) = \alpha\alpha' = A^2 - B^2 D.$$

Definition. Eine Funktion α des Körpers $\Omega = K(\sqrt{D})$ heißt „ganz", wenn sie einer Gleichung

$$\alpha^2 + A_1\alpha + A_2 = 0$$

mit ganz rationalem A_1 und A_2 genügt.

Es gilt der Satz:

Wenn α ganz und rational ist, so ist es ganz rational. Denn aus $\alpha = \frac{F}{G}$, wo F und G prim sind, folgt

$$F^2 + A_1 GF + A_2 G^2 = 0.$$

Also muß F^2 durch G teilbar sein, was nur geht, wenn G eine rationale Einheit ist. Dann ist aber α ganz rational.

Wenn aber α ganz und nicht rational ist, kann es nur einer quadratischen Gleichung der Form

$$\alpha^2 + A_1\alpha + A_2 = 0$$

genügen. Denn aus

$$\alpha^2 + B_1\alpha + B_2 = 0$$

folgte

$$(A_1 - B_1)\alpha + (A_2 - B_2) = 0,$$

was nur für $A_1 = B_1$ richtig sein kann, da sonst α doch rational wäre. Aus $A_1 = B_1$ folgt aber $A_2 = B_2$.

Gehen wir nun auf die Darstellung $\alpha = A + B\sqrt{D}$ und die zugehörige Gleichung

$$\alpha^2 - 2A\alpha + (A^2 - DB^2) = 0$$

zurück, so finden wir, wenn α rational ist, $B = 0$, also A ganz.

Wenn aber α nicht rational ist, muß die hingeschriebene Gleichung, da es dann nur eine dieser Form gibt, ganze rationale Koeffizienten haben. Es ist also $2A$ und demnach A ganz. Ferner ist $A^2 - DB^2$, also auch DB^2 ganz.

Wäre nun B nicht ganz, so bestünde sein Nenner aus mindestens einem Primfaktor, der im Nenner von B^2 quadratisch vorkäme und sich gegen D nicht heben könnte, da D nur einfache Primfaktoren besitzt. Also wäre DB^2 auch nicht ganz.

Ist umgekehrt A und B ganz, so ist ersichtlich $\alpha = A + B\sqrt{D}$ ganz.

Wir haben also:

Satz. Alle ganzen Funktionen des Körpers lassen sich in der Form $\alpha = X + Y\sqrt{D}$ darstellen, wo X und Y ganz sind.

Definition. Jedes Paar ω_1, ω_2 von ganzen Funktionen des Körpers heißt eine Basis, wenn sich alle ganzen Funktionen von Ω in der Form $X\omega_1 + Y\omega_2$ darstellen lassen.

Dann können wir also sagen:

Das Funktionspaar $1, \sqrt{D}$ bildet eine Basis.

Durch ein gleiches Verfahren wie in Zahlkörpern beweist man:

Jede Basis des Körpers hat die Form:

$$\left.\begin{aligned}\omega_1 &= A_1 + A_2\sqrt{D}\\ \omega_2 &= B_1 + B_2\sqrt{D}\end{aligned}\right\}, \quad \text{wo} \quad \begin{vmatrix} A_1 & A_2 \\ B_1 & B_2 \end{vmatrix} = a \text{ ist.}$$

Dabei ist A_1, A_2, B_1, B_2 ganz rational und a eine rationale Einheit.

Aus dem Multiplikationstheorem für Determinanten folgt sofort, wenn ω_1', ω_2' die Konjugierten der Basis ω_1, ω_2 sind:

$$\begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix}^2 = a_1^2 D_1, \quad \text{wo } a_1 \text{ eine Einheit ist.}$$

Man kann ersichtlich die Basis so wählen, daß a_1^2 ein beliebiger Rest, zum Beispiel 1 wird.

Aus diesem Grunde heißt D die Diskriminante des Körpers $K(\sqrt{D})$.

Aus der Basisdarstellung ergibt sich sofort, das Summe, Differenz und Produkt ganzer Funktionen aus Ω wieder ganz sind, daß mit α auch α' ganz ist, und daß $N(\alpha)$ ganz rational ist.

Definition. Eine ganze Funktion α heißt teilbar durch die ganze Funktion β, wenn sich ein γ (ganz) finden läßt, so daß $\alpha = \beta\gamma$ ist. β heißt auch Teiler von α.

Definition. Jeder Teiler der 1 heißt Einheit des Körpers.

Zu den Einheiten gehören also z. B. die rationalen Einheiten $1, 2, 3, \ldots, (p-1)$, die wir auch triviale Einheiten nennen wollen.

Es gilt der Satz:

Eine ganze Funktion ε ist dann und nur dann Einheit, wenn $N(\varepsilon)$ eine triviale Einheit ist.

Beweis. Aus $N(\varepsilon) = a = \varepsilon\varepsilon'$ folgt $\varepsilon' = \frac{a}{\varepsilon}$. Es ist also $\frac{a}{\varepsilon}$ und somit $\frac{1}{\varepsilon}$ ganz, d. h. ε eine Einheit.

Sei umgekehrt ε eine Einheit und $\varepsilon_1 = \frac{1}{\varepsilon}$, also $\varepsilon\varepsilon_1 = 1$. Dann ist auch $\varepsilon'\varepsilon_1' = 1$, also $N(\varepsilon)\cdot N(\varepsilon_1) = 1$. Die einzigen ganzen rationalen Teiler von 1 sind aber die trivialen Einheiten, so daß $N(\varepsilon) = a$ ist.

Ferner gilt ersichtlich:

Mit ε ist auch $\frac{1}{\varepsilon}$, ε' und $\frac{1}{\varepsilon'}$ eine Einheit.

Das Produkt zweier Einheiten ist selbst eine Einheit.

Definition. Zwei wechselseitig durcheinander teilbare ganze Funktionen α und β heißen assoziiert.

Dann sind also die beiden Quotienten $\frac{\alpha}{\beta}$ und $\frac{\beta}{\alpha}$ ganz, sind also Einheiten. Alle zu α assoziierten Funktionen sind also $\beta = \varepsilon\alpha$, wo ε irgendeine Körpereinheit ist.

Insbesondere sind alle Einheiten untereinander und mit 1 assoziiert.

§ 5.

Die Ideale.

Definition. Ein System ganzer Funktionen von $K(\sqrt{D})$ heißt ein Ideal, wenn mit den Funktionen α_1 und α_2 auch $\gamma_1\alpha_1 + \gamma_2\alpha_2$ zum Ideal gehört, wobei γ_1, γ_2 beliebige Funktionen des Körpers sind.

Satz. In jedem Ideal $\mathfrak{a}$ gibt es eine Basis. Darunter ist ein Funktionspaar ω_1, ω_2 zu verstehen, so daß man durch $X\omega_1 + Y\omega_2$ alle Funktionen des Ideals und nur diese erhält, falls X und Y alle ganzen rationalen Funktionen durchlaufen.

Beweis. Ist α eine Funktion aus $\mathfrak{a}$, so ist auch $\alpha' \cdot \alpha = N(\alpha)$ eine Funktion des Ideals. Im Ideal gibt es also ganze rationale Funktionen. T sei der größte gemeinsame Teiler aller ganz rationalen Funktionen aus $\mathfrak{a}$. Da dieser durch passende lineare Zusammensetzung erhalten werden kann, gehört er selbst dem Ideale an. Ebenso sei $R + S\sqrt{D}$ jene Idealfunktion, für die S der größte gemeinsame Teiler der Koeffizienten von $\sqrt{D}$ in den Idealfunktionen ist. Dann ist

$$\omega_1 = T, \qquad \omega_2 = R + S\sqrt{D}$$

eine Basis des Ideals.

Denn wenn $\alpha = A + B\sqrt{D}$ zu $\mathfrak{a}$ gehört, ist jedenfalls B durch S teilbar: $B = YS$. Mit α gehört auch $\alpha - Y\omega_2 = A - YR$ dem Ideale an. Als ganze rationale Funktion von $\mathfrak{a}$ ist sie durch T teilbar: $\alpha - Y\omega_2 = XT$. Demnach ist

$$\alpha = X\omega_1 + Y\omega_2.$$

Es ist also ω_1, ω_2 eine Basis.

Gleichzeitig haben wir erkannt, daß die Basis stets in der speziellen Form

$$\omega_1 = T, \qquad \omega_2 = R + S\sqrt{D}$$

wählbar ist.

Man erkennt auch leicht, daß $|R| < |T|$ angenommen werden darf. Diese Form der Basis nennen wir die *adaptierte*. T und S sind in ihr

bis auf triviale Einheiten als Faktor eindeutig bestimmt. Nimmt man die Bedingung $|R| < |T$ hinzu, so ist mit der Wahl von S auch R eindeutig festgelegt. Denn wenn $R + S\sqrt{D}$ und $R_1 + S\sqrt{D}$ dem Ideal angehören mit $|R| < |T|$ und $|R_1| < |T|$, so gehört auch $R - R_1$ dem Ideal an und ist durch T teilbar. Da $|R - R_1| < |T|$ ist, muß $R = R_1$ sein.

Wir beweisen nun den

Satz. Die notwendige und hinreichende Bedingung dafür, daß $\omega = T$, $\omega_2 = R + S\sqrt{D}$ die Basis eines Ideals bildet, lautet: Es muß gelten

$$T = 2CS, \quad R = BS, \quad \frac{B^2 - D}{2C} = 2A,$$

wo A, B, C ganze rationale Funktionen sind. Die Basis hat also die Form

$$\omega_1 = 2CS, \quad \omega_2 = S(B + \sqrt{D}), \quad \text{wo} \quad D = B^2 - 4AC,$$

und umgekehrt ist dann ω_1, ω_2 Basis eines Ideals.

Beweis: 1. Mit $\omega_1 = T$ gehört auch $\omega_1\sqrt{D} = T\sqrt{D}$ zum Ideal, muß sich also durch die Basis darstellen lassen:

$$T\sqrt{D} = \omega_1 X + \omega_2 Y = TX + RY + SY\sqrt{D}.$$

Also:

$$T = SY \quad \text{oder,} \quad Y = 2C \text{ gesetzt,} \quad T = 2CS.$$

Nun muß sein

$$TX + RY = 0,$$

oder nach dem eben gezeigten

$$SYX + RY = 0.$$

Da $T \neq 0$, also $Y \neq 0$ ist, muß sein

$$R = -SX \quad \text{oder,} \quad X = -B \text{ gesetzt,} \quad R = BS.$$

Mit $\omega_2 = S(B + \sqrt{D})$ gehört auch $\omega_2(B - \sqrt{D}) = S(B^2 - D)$ zum Ideal. Es muß durch $T = 2CS$ teilbar sein, also ist $\frac{B^2 - D}{2C}$ ganz. Unsere Bedingungen sind also notwendig.

2. Daß die Bedingungen hinreichen, zeigen wir so. Sei

$$\omega_1 = 2CS, \quad \omega_2 = S(B + \sqrt{D}) \quad \text{und} \quad B^2 - D = 4AC.$$

Die Menge der Funktionen $\gamma_1\omega_1 + \gamma_2\omega_2$, wo γ_1 und γ_2 irgendwelche ganze Funktionen aus $K(\sqrt{D})$ sind, bilden offenbar ein Ideal $\mathfrak{a}$. Jede Zahl α aus $\mathfrak{a}$ hat die Form

$$\begin{aligned}\alpha &= (X + Y\sqrt{D})\,\omega_1 + (X_1 + Y_1\sqrt{D})\,\omega_2 \\ &= S(2CX + BX_1 + Y_1 D) + S(2CY + BY_1 + X_1)\sqrt{D} \\ &= S(2CX + BX_1 + Y_1 D - 2CBY - B^2 Y_1 - BX_1) \\ &\qquad + S(2CY + BY_1 + X_1)\cdot(B + \sqrt{D}) \\ &= 2CS(X - 2AY_1 - BY) + (2CY + BY_1 + X_1)\cdot S(B + \sqrt{D}) \\ &= X_2\omega_1 + Y_2\omega_2,\end{aligned}$$

wo X_2 und Y_2 ganz rational sind. ω_1, ω_2 sind also eine Basis von $\mathfrak{a}$.

Die Basis eines jeden Ideals hat also (wenn sie adaptiert ist) die Form $\omega_1 = 2CS$, $\omega_2 = S\cdot(B + \sqrt{D})$, wo $D = B^2 - 4AC$ ist. C und S sind dabei bis auf triviale Einheitsfaktoren bestimmt. Nimmt man noch $|B| < |C|$ hinzu, so ist auch B vollkommen eindeutig festgelegt.

Satz. Die ganzen rationalen Funktionen A, B, C haben keinen gemeinsamen Teiler.

Es folgt dies aus $D = B^2 - 4AC$ und daraus, daß D keinen quadratischen Teiler hat. Denn einen solchen müßte es geben, wenn ein gemeinsamer Primfaktor von A und C auch in B aufginge.

Wenn ein Ideal $\mathfrak{a}$ aus den Funktionen $\alpha_1, \alpha_2, \ldots, \alpha_n$ so gebildet ist, daß jede Funktion α aus $\mathfrak{a}$ die Form

$$\alpha = \lambda_1\alpha_1 + \lambda_2\alpha_2 + \ldots + \lambda_n\alpha_n \quad (\lambda_\nu \text{ ganze Körperfunktionen})$$

hat, und umgekehrt jede Funktion dieser Form zu $\mathfrak{a}$ gehört, so schreiben wir:

$$\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Ersichtlich gilt, wenn ω_1, ω_2 eine Basis ist,

$$\mathfrak{a} = (\omega_1, \omega_2).$$

Jedes Ideal läßt sich also durch höchstens zwei Funktionen aufbauen.

Aus jeder ganzen Funktion α bilden wir das Ideal (α), bestehend aus der Gesamtheit aller durch α teilbaren Funktionen von $K(\sqrt{D})$. Diese Ideale heißen Hauptideale.

Insbesondere ist das System aller ganzen Funktionen des Körpers ein Hauptideal, das Hauptideal (1).

Wir erkennen wieder, daß assoziierte Funktionen und nur diese dasselbe Hauptideal erzeugen. Aus diesem Grunde lassen wir oft bei Hauptidealen die Klammern weg und schreiben kurz α statt (α).

Von den Basen eines Ideals zeigt man leicht:

Satz. Sind ω_1, ω_2 und ω_1^*, ω_2^* zwei Basen des Ideals $\mathfrak{a}$, so ist

$$\left.\begin{aligned}\omega_1^* &= A_1\omega_1 + A_2\omega_2 \\ \omega_2^* &= B_1\omega_1 + B_2\omega_2\end{aligned}\right\} \text{ mit } \begin{vmatrix} A_1 & A_2 \\ B_1 & B_2 \end{vmatrix} = a,$$

wo a eine Einheit ist.

Dies hat zur Folge, daß $\begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix}^2$ bis auf einen quadratischen Rest als Faktor von der Wahl der Basis unabhängig ist und nur vom Ideal abhängt. Die adaptierte Basis ergibt dafür den Wert $(4CS^2)^2 D$. Wir können also setzen

$$\begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix}^2 = a^2 (N\mathfrak{a})^2 \cdot D,$$

wo a^2 ein quadratischer Rest und $N\mathfrak{a}$ ganz rational primär ist.

$N\mathfrak{a}$ heißt die Norm des Ideals $\mathfrak{a}$, ihr Betrag $|N\mathfrak{a}|$ die absolute Norm.

Für $N\mathfrak{a}$ ergibt die adaptierte Basis den Wert

$$N\mathfrak{a} = a_1 \cdot CS^2,$$

wo a_1 eine passende rationale Einheit ist; und zwar wird, da $\operatorname{sgn} N\mathfrak{a} = 1$ ist,

$$N\mathfrak{a} = \frac{CS^2}{\operatorname{sgn} CS^2}.$$

Definition. Sind $\mathfrak{a}$ und $\mathfrak{b}$ zwei Ideale, so ist die Menge der Funktionen $\Sigma \gamma \cdot \alpha\beta$, wo α und β Funktionen von $\mathfrak{a}$ bzw. $\mathfrak{b}$, γ aber beliebige Körperfunktionen sind, ein Ideal $\mathfrak{c}$, welches das Produkt von $\mathfrak{a}$ und $\mathfrak{b}$ genannt werde:

$$\mathfrak{c} = \mathfrak{a}\mathfrak{b}.$$

Es gilt, wie man leicht erkennt,

$$\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a} \quad \text{und} \quad (\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c}).$$

Für Hauptideale findet man

$$(\alpha) \cdot (\beta) = (\alpha\beta)$$

und

$$(\alpha) \cdot (\beta_1, \beta_2, \ldots, \beta_n) = (\alpha\beta_1, \alpha\beta_2, \ldots, \alpha\beta_n).$$

Also ist

$$\mathfrak{a} \cdot (1) = \mathfrak{a}.$$

Endlich gilt, wenn $\mathfrak{a} = (\alpha_1, \alpha_2)$ und $\mathfrak{b} = (\beta_1, \beta_2)$ ist,

$$\mathfrak{a} \cdot \mathfrak{b} = (\alpha_1\beta_1, \alpha_1\beta_2, \alpha_2\beta_1, \alpha_2\beta_2).$$

Definition. Ersetzt man in einem Ideal $\mathfrak{a}$ alle Funktionen durch ihre Konjugierten, so entsteht wieder ein Ideal $\mathfrak{a}'$, welches das zu $\mathfrak{a}$ konjugierte Ideal genannt werde.

Ist ω_1, ω_2 eine Basis von $\mathfrak{a}$, so ist ω_1', ω_2' eine Basis von $\mathfrak{a}'$.

Das konjugierte Ideal zu $\mathfrak{a}\mathfrak{b}$ ist $\mathfrak{a}'\mathfrak{b}'$.

Endlich: Ist $\mathfrak{a} = (\alpha, \beta)$, so ist $\mathfrak{a}' = (\alpha', \beta')$.

Definition. Ein mit seinem konjugierten identisches Ideal, für welches also $\mathfrak{a} = \mathfrak{a}'$ ist, heißt ambiges Ideal.

Satz. Es ist $\mathfrak{a}\cdot\mathfrak{a}' = (N\mathfrak{a})$ also ein Hauptideal.

Beweis. Sei

$$\omega_1 = 2CS, \quad \omega_2 = S(B+\sqrt{D}), \quad D = B^2 - 4AC$$

die adaptierte Basis von $\mathfrak{a}$. Dann ist:

$$\begin{aligned}\mathfrak{a}\cdot\mathfrak{a}' &= (2CS,\ S(B+\sqrt{D}))\cdot(2CS,\ S(B-\sqrt{D}))\\ &= (S^2)\,(2C,\ B+\sqrt{D})\,(2C,\ B-\sqrt{D})\\ &= (S^2)\,(4C^2,\ 2CB+2C\sqrt{D},\ 2CB-2C\sqrt{D},\ B^2-D)\\ &= (S^2)\,(C^2,\ CB,\ AC,\ C\sqrt{D})\\ &= (C\cdot S^2)\cdot(A,\ B,\ C,\ \sqrt{D}).\end{aligned}$$

Da nun A, B, C keinen gemeinsamen Teiler haben, kommt im letzten Ideal (1) vor. Es ist also

$$\mathfrak{a}\cdot\mathfrak{a}' = (C\cdot S^2)\cdot(1) = (N\mathfrak{a}).$$

Hieraus folgern wir:

Satz. Die Norm des Produktes zweier Ideale ist gleich dem Produkt ihrer Normen. Denn es ist

$$(N(\mathfrak{a}\mathfrak{b})) = (\mathfrak{a}\mathfrak{b})\cdot(\mathfrak{a}\mathfrak{b})' = \mathfrak{a}\mathfrak{a}'\cdot\mathfrak{b}\mathfrak{b}' = (N(\mathfrak{a})\cdot N(\mathfrak{b})).$$

Daher ist $N(\mathfrak{a}\mathfrak{b})$ assoziiert mit $N\mathfrak{a}\cdot N\mathfrak{b}$. Da beide rational und primär sind, gilt also

$$N(\mathfrak{a}\mathfrak{b}) = N\mathfrak{a}\cdot N\mathfrak{b}.$$

Ebenso erhält man:

Satz. Die Norm eines Hauptideals ist, bis auf eine triviale Einheit als Faktor, gleich der Norm der zugehörigen Funktion.

Wie man sieht, laufen die Schlüsse denen im Zahlkörper vollkommen parallel. Es wird also genügen, die weiteren Definitionen und Sätze anzuführen.

Definition. Ist α eine Funktion des Ideals $\mathfrak{a}$, so schreiben wir

$$\alpha \equiv 0 \pmod{\mathfrak{a}}.$$

Ebenso besagt

$$\alpha \equiv \beta \pmod{\mathfrak{a}},$$

daß $\alpha - \beta$ eine Funktion aus $\mathfrak{a}$ ist.

Satz I. Aus $(\gamma)\cdot\mathfrak{a} = (\gamma)\cdot\mathfrak{b}$ folgt $\mathfrak{a} = \mathfrak{b}$.

Satz II. Aus $\mathfrak{a}\cdot\mathfrak{c} = \mathfrak{b}\cdot\mathfrak{c}$ folgt $\mathfrak{a} = \mathfrak{b}$.

Definitionen. 1. Ist $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, so heißt $\mathfrak{a}$ teilbar durch $\mathfrak{b}$ und $\mathfrak{b}$ ein Teiler von $\mathfrak{a}$.

2. Ein Ideal, welches nur durch (1) und sich selbst teilbar ist, heißt Primideal. (Dabei soll es von (1) verschieden sein.)

Weiter haben wir die Sätze:

III. Ist $\mathfrak{b}$ Teiler von $\mathfrak{a}$ und $\alpha \equiv 0 \pmod{\mathfrak{a}}$, so gilt auch $\alpha \equiv 0 \pmod{\mathfrak{b}}$.

IV. Ein Ideal $\mathfrak{a}$ hat nur endlich viele Teiler.

V. Wenn für jede Funktion β des Ideals $\mathfrak{b}$ gilt $\beta \equiv 0 \pmod{\mathfrak{a}}$, so ist $\mathfrak{b}$ durch $\mathfrak{a}$ teilbar, und umgekehrt. Insbesondere heißt also $\alpha \equiv 0 \pmod{\mathfrak{a}}$: Das Hauptideal (α) ist durch $\mathfrak{a}$ teilbar.

VI. Sind $\mathfrak{a}$ und $\mathfrak{b}$ zwei Ideale, so hat das Ideal $\mathfrak{d}$, welches durch Vereinigung der Funktionen von $\mathfrak{a}$ und $\mathfrak{b}$ gebildet ist, alle Eigenschaften des größten gemeinsamen Teilers von $\mathfrak{a}$ und $\mathfrak{b}$ und ist durch diese eindeutig bestimmt. Es heißt deshalb auch der größte gemeinsame Teiler von $\mathfrak{a}$ und $\mathfrak{b}$: $\mathfrak{d} = (\mathfrak{a}, \mathfrak{b})$.

Wenn $(\mathfrak{a}, \mathfrak{b}) = (1)$ ist, heißen die Ideale $\mathfrak{a}$ und $\mathfrak{b}$ relativ prim. Dann gibt es also aus $\mathfrak{a}$ und $\mathfrak{b}$ je eine Funktion α und β so, daß $\alpha + \beta = 1$ ist.

VII. Wenn das Produkt $\mathfrak{a}\mathfrak{b}$ zweier Ideale durch das Primideal $\mathfrak{p}$ teilbar ist, muß einer der Faktoren durch $\mathfrak{p}$ teilbar sein.

Nunmehr kann der Hauptsatz über die Eindeutigkeit der Zerlegung in Primideale leicht erschlossen werden.

Satz. Jedes Ideal $\mathfrak{a}$ läßt sich auf eine, und bis auf die Anordnung auch nur auf eine Weise in Primideale zerlegen.

Beweis. Wenn $\mathfrak{a}$ nicht selbst Primideal ist, läßt es sich als Produkt zweier Ideale darstellen. Auf diese werde die Betrachtung erneut angewendet. Nach IV muß dies einmal abbrechen, wodurch man die gewünschte Zerlegung erhält:

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n.$$

Aus VII erschließt man die Identität zweier gegebener Zerlegungen.

§ 6.

Primideale.

Satz. Jedes Primideal $\mathfrak{p}$ geht in einer und nur einer rationalen Primfunktion P auf. (Gemeint ist natürlich das Hauptideal (P).)

Beweis. Da $\mathfrak{p}\mathfrak{p}' = N\mathfrak{p}$ ist, erkennen wir, wenn $N\mathfrak{p} = P_1 P_2 \dots P_r$ die Zerlegung von $N\mathfrak{p}$ in Primfunktionen ist, aus $\mathfrak{p}\mathfrak{p}' = P_1 P_2 \dots P_r$, daß $\mathfrak{p}$ in wenigstens einer der Primfunktionen rechterhand aufgeht.

Ist andrerseits $P \equiv 0 \pmod{\mathfrak{p}}$ und $Q \equiv 0 \pmod{\mathfrak{p}}$, wo P und Q verschiedene Primfunktionen sind, so ist auch 1 Funktion von $\mathfrak{p}$, da ja P und Q relativ prim sind. Das geht nicht.

Um alle Primideale zu erhalten, genügt es also alle primären Primfunktionen P zu zerlegen.

Es gehe $\mathfrak{p}$ auf in P:

$$P = \mathfrak{p} \cdot \mathfrak{a},$$

also

$$N(P) = P^2 = N\mathfrak{p} \cdot N\mathfrak{a}.$$

Es kann also nur entweder $N\mathfrak{p} = P$ oder $N\mathfrak{p} = P^2$ sein.

Sei nun $\omega_1 = 2CS$, $\omega_2 = S(B + \sqrt{D})$ eine Basis von $\mathfrak{p}$, wobei C und S primär sind. Dann gilt

$$N\mathfrak{p} = CS^2.$$

1. Die Kongruenz $X^2 \equiv D \pmod{P}$ sei unlösbar. Dann kann C nicht den Wert P haben, da ja für alle $B: (B^2 - D)$ durch P nicht teilbar ist. Wegen $CS^2 = P$ oder P^2 muß also $C = 1$ und $S = P$ sein, also $N\mathfrak{p} = P^2$. Da man $|B| < |C|$ annehmen kann, ist $B = 0$, also

$$\mathfrak{p} = (2P, P\sqrt{D}) = (P) \cdot (1, \sqrt{D}) = (P).$$

P ist also unzerlegbar, somit selbst Primideal.

2. Es sei die Kongruenz $X^2 \equiv D \pmod{P}$ lösbar.

a) P sei prim zu D; B eine Lösung der Kongruenz. Dann ist auch B prim zu P. Wir bilden das Ideal $\mathfrak{p}$ mit der Basis $\omega_1 = P$, $\omega_2 = B + \sqrt{D}$, wo also $S = 1$, $2C = P$ ist. Das geht, da $\frac{B^2 - D}{2C} = \frac{B^2 - D}{P}$ ganz ist. Es ist dann

$$\mathfrak{p} = (P, B + \sqrt{D}), \qquad \mathfrak{p}' = (P, B - \sqrt{D}), \qquad N\mathfrak{p} = P.$$

Wegen $N\mathfrak{p} = P$ ist $\mathfrak{p}$ sicher ein Primideal, und zwar ist $N\mathfrak{p} = \mathfrak{p}\mathfrak{p}' = P$. Ferner ist $\mathfrak{p}$ und $\mathfrak{p}'$ verschieden, denn ihr größter gemeinsamer Teiler ist

$$(P, B + \sqrt{D}, B - \sqrt{D}) = (P, B, \sqrt{D}) = (1).$$

P ist dann also das Produkt zweier verschiedener Primideale $\mathfrak{p}$ und $\mathfrak{p}'$, deren Norm P ist.

b) P sei ein Teiler von D, also $D = PD'$, wo D' prim zu P ist, da D keine quadratischen Teiler enthält. Wir bilden das Ideal $\mathfrak{p}$ mit der Basis $\omega_1 = P$, $\omega_2 = \sqrt{D}$, so daß also $S = 1$, $2C = P$, $B = 0$ ist. Dann ist $\frac{B^2 - D}{2C} = -\frac{D}{P} = D'$ ganz. Wir haben

$$\mathfrak{p} = (P, \sqrt{D}) = \mathfrak{p}', \qquad N\mathfrak{p} = P = \mathfrak{p}\mathfrak{p}' = \mathfrak{p}^2.$$

Es ist also $\mathfrak{p}$ ein Primideal und sein Quadrat gleich P.

Führen wir mit Dedekind das Symbol $\left[\frac{D}{P}\right]$ ein (analog zum Legendreschen, welches $\left(\frac{a}{p}\right)$ geschrieben werde), welches ± 1 sei, je nachdem die Kongruenz $X^2 \equiv D \pmod{P}$ lösbar oder unlösbar ist, und wo D und P relativ prim seien, so haben wir bewiesen:

Satz. 1. Ist P Teiler der Diskriminante D, so ist P das Quadrat eines Primideals

$$P = \mathfrak{p}^2, \quad \text{wo} \quad \mathfrak{p} = (P, \sqrt{D})$$

die Basisdarstellung von $\mathfrak{p}$ ist.

2. Ist P prim zu D und $\left[\frac{D}{P}\right] = +1$, so zerfällt P in das Produkt zweier verschiedener konjugierter Primideale

$$P = \mathfrak{p} \cdot \mathfrak{p}', \quad \text{wo} \quad \mathfrak{p} = (P, B + \sqrt{D}), \quad \mathfrak{p}' = (P, B - \sqrt{D})$$

ihre Basisdarstellung ist, und B eine Wurzel der Kongruenz

$$X^2 \equiv D \pmod{P}.$$

3. Ist P prim zu D und $\left[\frac{D}{P}\right] = -1$, so ist P selbst Primideal und

$$P = (P, P\sqrt{D})$$

seine Basisdarstellung.

Als ambig erkennt man also nur die Primideale der Fälle 1 und 3. Sei nun $\mathfrak{a}$ ein ambiges Ideal $\mathfrak{a} = \mathfrak{a}'$. Mit jedem Primideal $\mathfrak{p}$ geht also auch $\mathfrak{p}'$ in $\mathfrak{a}$ auf. Entweder also geht $\mathfrak{p} \cdot \mathfrak{p}'$ in $\mathfrak{a}$ auf (rationaler Teiler), oder aber $\mathfrak{p}$ ist selbst ambig $\mathfrak{p} = \mathfrak{p}'$. Ziehen wir alle rationalen Teiler zusammen, so erhalten wir also

$$\mathfrak{a} = (A) \cdot \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \dots \mathfrak{p}_r,$$

wo A ganz rational ist, und $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r$ verschiedene Primideale des Falles 1 sind. Denn Fall 3 liefert ja rationale Faktoren.

Wir erwähnen noch eine Reihe von Sätzen, deren Beweis man an der Hand der üblichen Beweise leicht konstruieren kann.

Werden nämlich die Funktionen des Körpers in Klassen geteilt, so daß in eine Restklasse alle modulo $\mathfrak{a}$ einander kongruenten Funktionen zu liegen kommen, so gilt:

Satz. Die Anzahl der Restklassen modulo $\mathfrak{a}$, also die Anzahl der einander inkongruenten Funktionen des Körpers, ist gleich der absoluten Norm von $\mathfrak{a}$, also gleich $|N\mathfrak{a}|$.

Faßt man nur die primen Restklassen ins Auge (welche eine Gruppe bilden), so gilt, wenn ihre Anzahl mit $\Phi_D(\mathfrak{a})$ bezeichnet wird:

I. Ist $\mathfrak{a}$ prim zu $\mathfrak{b}$, so ist $\Phi_D(\mathfrak{a}\mathfrak{b}) = \Phi_D(\mathfrak{a}) \cdot \Phi_D(\mathfrak{b})$.

II. Ist $\mathfrak{a} = \mathfrak{p}_1^{n_1} \mathfrak{p}_2^{n_2} \dots \mathfrak{p}_r^{n_r}$ die Zerlegung von $\mathfrak{a}$ in Primideale, so gilt

$$\Phi_D(\mathfrak{a}) = |N\mathfrak{a}| \cdot \left(1 - \frac{1}{N\mathfrak{p}_1}\right)\left(1 - \frac{1}{N\mathfrak{p}_2}\right) \dots \left(1 - \frac{1}{N\mathfrak{p}_r}\right),$$

für Primideale also speziell:

$$\Phi_D(\mathfrak{p}) = |N\mathfrak{p}| - 1.$$

Aus der Gruppeneigenschaft der primen Restklassen folgt der Fermatsche Satz:

III. Ist α prim zu $\mathfrak{a}$, so gilt

$$\alpha^{\Phi_D(\mathfrak{a})} \equiv 1 \pmod{\mathfrak{a}}.$$

Ist also $\mathfrak{a} = \mathfrak{p}$ ein Primideal, so gilt für jede nicht durch $\mathfrak{p}$ teilbare Funktion α

$$\alpha^{|N\mathfrak{p}|-1} \equiv 1 \pmod{\mathfrak{p}}.$$

IV. Eine Kongruenz nach einem Primideal als Modul kann nicht mehr inkongruente Wurzeln haben, als ihr Grad beträgt.

V. Die Anzahl der zum Teiler d von $(|N\mathfrak{p}|-1)$ als Exponent gehörigen primen Restklassen mod $\mathfrak{p}$ ist $\varphi(d)$, wo $\varphi(d)$ die elementare Eulersche Funktion ist.

VI. Die Anzahl der Primitivfunktionen nach einem Primideal $\mathfrak{p}$ beträgt

$$\varphi(|N\mathfrak{p}|-1).$$

§ 7.

Die Idealklassen des Körpers.

Definition. Zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ heißen äquivalent, wenn es zwei ganze Funktionen des Körpers, α und β, gibt, so daß

$$(\beta)\cdot\mathfrak{a} = (\alpha)\cdot\mathfrak{b}$$

ist. Wir schreiben:

$$\mathfrak{a} \sim \mathfrak{b}.$$

Die Äquivalenzbeziehung können wir symbolisch auch so ausdrücken:

$$\frac{\mathfrak{a}}{\mathfrak{b}} = \frac{\alpha}{\beta} = \varrho,$$

wo ϱ eine, bis auf eine willkürliche Körpereinheit feste (nicht notwendig ganze) Funktion des Körpers ist. Denn aus $(\beta_1)\mathfrak{a} = (\alpha_1)\mathfrak{b}$ folgt durch Multiplikation mit (β), daß $(\beta_1)(\alpha) = (\alpha_1)(\beta)$ oder $\alpha\beta_1 = \alpha_1\beta\varepsilon$, wo ε eine Einheit ist. Also:

$$\frac{\alpha}{\beta} = \frac{\alpha_1}{\beta_1}\varepsilon.$$

Sofort erkennen wir die Richtigkeit folgender Behauptungen:

1. Aus $\mathfrak{a} \sim \mathfrak{b}$ und $\mathfrak{b} \sim \mathfrak{c}$ folgt $\mathfrak{a} \sim \mathfrak{c}$.
2. Aus $\mathfrak{a} \sim \mathfrak{b}$ und $\mathfrak{c} \sim \mathfrak{d}$ folgt $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{d}$.
3. Aus $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{d}$ und $\mathfrak{a} \sim \mathfrak{b}$ folgt $\mathfrak{c} \sim \mathfrak{d}$.
4. Aus $\mathfrak{a} \sim \mathfrak{b}$ folgt $\mathfrak{a}' \sim \mathfrak{b}'$.

5. Mit (1) sind die Hauptideale und nur diese äquivalent.

6. Wenn $\frac{\mathfrak{a}}{\mathfrak{b}} = \varrho$ und ω_1, ω_2 eine Basis von $\mathfrak{b}$ ist, so ist $\varrho\omega_1$, $\varrho\omega_2$ eine Basis von $\mathfrak{a}$.

Beweis. Sei $(\beta)\mathfrak{a} = (\alpha)\mathfrak{b}$ und $\varrho = \frac{\alpha}{\beta}$. β_1 sei eine Funktion aus $\mathfrak{b}$, also $\alpha\beta_1$ eine Funktion aus $(\beta)\mathfrak{a}$. Es ist also $\frac{\alpha\beta_1}{\beta}$ ganz, so daß $\varrho\beta_1$ ganz ist und zwar zu $\mathfrak{a}$ gehört. Also sind $\varrho\omega_1$ und $\varrho\omega_2$ ganz und Funktionen von $\mathfrak{a}$. Also auch jedes $X\cdot(\varrho\omega_1) + Y(\varrho\omega_2)$. Wenn nun α zu $\mathfrak{a}$ gehört, ist $\frac{\alpha}{\varrho}$ ganz und zu $\mathfrak{b}$ gehörig. Also gilt

$$\frac{\alpha}{\varrho} = X\omega_1 + Y\omega_2,$$

somit

$$\alpha = X\cdot\varrho\omega_1 + Y\cdot\varrho\omega_2.$$

Auf Grund von 1 können wir sagen:

Alle untereinander äquivalenten Ideale liegen in einer Klasse, einer Idealklasse $\mathfrak{K}$ des Körpers.

Nach 5 bilden insbesondere die Hauptideale eine Klasse, die Hauptklasse $\mathfrak{K}_0$. In ihr liegt das Ideal (1).

Wegen 2 können wir definieren:

Das Produkt $\mathfrak{K}_1\mathfrak{K}_2$ der beiden Idealklassen $\mathfrak{K}_1$ und $\mathfrak{K}_2$ ist jene Klasse, welche die Produkte der Ideale aus $\mathfrak{K}_1$ mit jener aus $\mathfrak{K}_2$ enthält: $\mathfrak{K}_3 = \mathfrak{K}_1\mathfrak{K}_2$.

Die Multiplikation der Idealklassen ist ersichtlich kommutativ und assoziativ. Für die Hauptklasse $\mathfrak{K}_0$ gilt $\mathfrak{K}\mathfrak{K}_0 = \mathfrak{K}$, wenn $\mathfrak{K}$ irgendeine Klasse ist.

Aus 4 folgt, daß die Ideale, welche zu jenen einer Idealklasse $\mathfrak{K}$ konjugiert sind, auch eine Idealklasse bilden, welche durch einen Akzent gekennzeichnet werde: $\mathfrak{K}'$.

Dann ergibt sich aus $\mathfrak{a}\mathfrak{a}' = (N\mathfrak{a})$, daß $\mathfrak{K}\mathfrak{K}' = \mathfrak{K}_0$, wo $\mathfrak{K}_0$ die Hauptklasse ist.

Punkt 3 kann so geschrieben werden: Aus $\mathfrak{K}_1\mathfrak{K}_2 = \mathfrak{K}_1\mathfrak{K}_3$ folgt $\mathfrak{K}_2 = \mathfrak{K}_3$.

Endlich können wir in der Gleichung $\mathfrak{K}_1\mathfrak{K}_2 = \mathfrak{K}_3$ irgend zwei Klassen beliebig vorschreiben, wodurch dann die dritte eindeutig bestimmt ist.

In der Tat folgt, wenn etwa $\mathfrak{K}_1$ und $\mathfrak{K}_3$ gegeben sind, aus $\mathfrak{K}_1\mathfrak{K}_2 = \mathfrak{K}_3$ durch Multiplikation mit $\mathfrak{K}_1'$:

$$\mathfrak{K}_2 = \mathfrak{K}_1'\mathfrak{K}_3,$$

und umgekehrt ist dann auch

$$\mathfrak{K}_1\mathfrak{K}_2 = \mathfrak{K}_3.$$

Aus dem Bisherigen folgt, daß die Idealklassen eine Abelsche Gruppe bilden.

Dabei ist $\mathfrak{K}_0$ das Einheitselement und $\mathfrak{K}'$ das zu $\mathfrak{K}$ inverse: $\mathfrak{K}^{-1} = \mathfrak{K}'$.

Eine Idealklasse heißt ambig, wenn $\mathfrak{K} = \mathfrak{K}'$ ist (oder $\mathfrak{K} = \mathfrak{K}^{-1}$ oder $\mathfrak{K}^2 = \mathfrak{K}_0$).

Unser nächstes Ziel ist nun, die Endlichkeit der Anzahl der Idealklassen, die wir mit h bezeichnen, nachzuweisen.

§ 8.

Äquivalente Funktionen.

Es sei $\omega = X + Y\sqrt{\Delta}$ (X, Y rational, Δ quadratfrei und $\operatorname{sgn}\Delta = 1$ oder g) eine quadratische Irrationalität. Dann genügen ω und seine Konjugierte $\omega' = X - Y\sqrt{\Delta}$ der Gleichung

$$\omega^2 - 2X\omega + (X^2 - \Delta Y^2) = 0.$$

Setzen wir

$$X^2 - \Delta Y^2 = \frac{A}{C}, \qquad 2X = \frac{B}{C},$$

wo A, B, C ganz und ohne gemeinsamen Teiler seien. Die drei Funktionen sind dann bis auf einen rationalen Einheitsfaktor eindeutig bestimmt. Die Gleichung für ω lautet:

$$C\omega^2 + A = B\omega.$$

Die Diskriminante $B^2 - 4AC$ dieser Gleichung werde nun mit D bezeichnet (D braucht also hier nicht gerade quadratfrei zu sein). D ist dann bis auf einen quadratischen Rest als Faktor festgelegt.

Um nun die Einheitsfaktoren zu normieren, sei zunächst das Vorzeichen von $\sqrt{\Delta}$ so gewählt, daß entweder $\sqrt{\Delta}$ selbst, oder $\frac{1}{\sqrt{g}}\sqrt{\Delta}$, $\frac{1}{\sqrt{t}}\sqrt{\Delta}$, bzw. $\frac{1}{\sqrt{gt}}\sqrt{\Delta}$ primär ist.

Nun findet man leicht $D = 4C^2Y^2\Delta$.

Da Δ quadratfrei ist, muß wieder, wie schon früher einmal, $4C^2Y^2$, also $2CY$ ganz sein.

Der A, B, C gemeinsame willkürliche Einheitsfaktor werde nun so gewählt, daß $\operatorname{sgn}(2CY) = +1$ ist. Dann ist

$$\operatorname{sgn} D = \operatorname{sgn}\Delta.$$

Nun setzen wir noch fest:

$$\sqrt{D} = 2CY\cdot\sqrt{\Delta}, \quad \text{also} \quad Y\sqrt{\Delta} = \frac{\sqrt{D}}{2C}.$$

Auf diese Art sind ω und die Funktionen A, B, C eindeutig aufeinander bezogen. Wir schreiben:

$$\omega = \{A, B, C\} = \frac{B+\sqrt{D}}{2C},$$

wobei zum Beispiel:

$$\omega' \quad \{-A, -B, -C\} = \frac{B-\sqrt{D}}{2C}.$$

Und zwar ist die Beziehung umkehrbar eindeutig.

Definition. Zwei Funktionen $\omega = \{A, B, C\}$ und $\omega_1 = \{A_1 B_1 C_1\}$ heißen äquivalent, wenn sie miteinander durch eine Beziehung der Form verknüpft sind,

$$\omega_1 = \frac{\alpha\omega+\beta}{\gamma\omega+\delta} \quad \text{mit} \quad \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = a,$$

wo α, β, γ, δ ganz rational sind, und a eine triviale Einheit ist.

Ohne weiteres zeigt man:

Aus $\omega \sim \omega_1$ und $\omega_1 \sim \omega_2$ folgt $\omega \sim \omega_2$.

Aus $\omega \sim \omega_1$ folgt $\omega_1 \sim \omega$.

Durch die Äquivalenzdefinition zerfallen also die Funktionen in Klassen.

Wir haben nun die Transformation der Funktionen A, B, C herzuleiten. Sei

$$\omega = X + Y\sqrt{\Delta}, \qquad \omega_1 = X_1 + Y_1\sqrt{\Delta}.$$

Dann ist

$$X_1 + Y_1\sqrt{\Delta} = \frac{\alpha X+\beta+\alpha Y\sqrt{\Delta}}{\gamma X+\delta+\gamma Y\sqrt{\Delta}},$$

also

$$Y_1 = \frac{-(\alpha X+\beta)\gamma Y+(\gamma X+\delta)\alpha Y}{(\gamma X+\delta)^2-\gamma^2 Y^2\Delta} = \frac{aY}{\gamma^2(X^2-Y^2\Delta)+2X\gamma\delta+\delta^2}.$$

Nach Einführung von A, B, C wird daraus

$$\text{(I)} \qquad aYC = (A\gamma^2+B\gamma\delta+C\delta^2)\cdot Y_1.$$

Aus $C\omega^2+A = B\omega$ erhält man für ω_1 wegen $\omega = \frac{\delta\omega_1-\beta}{-\gamma\omega_1+\alpha}$ die Beziehung

$$C(\delta\omega_1-\beta)^2+A(-\gamma\omega_1+\alpha)^2 = B(\delta\omega_1-\beta)(-\gamma\omega_1+\alpha)$$

oder

$$\begin{aligned}(A\gamma^2+B\gamma\delta+C\delta^2)\omega_1^2+(A\alpha^2+B\alpha\beta+C\beta^2)\\ = (2A\alpha\gamma+B(\alpha\delta+\beta\gamma)+2C\beta\delta)\omega_1.\end{aligned}$$

Vergleicht man dies mit $C_1\omega_1^2+A_1 = B_1\omega_1$, so erhellt, daß sich die Koeffizienten der beiden Gleichungen nur um einen Faktor unterscheiden können. Ich behaupte, daß dieser Faktor a ist, daß also

$$\left.\begin{aligned}
(1)\quad & aA_1 = A\alpha^2 + B\alpha\beta + C\beta^2,\\
(2)\quad & aB_1 = 2A\alpha\gamma + B(\alpha\delta + \gamma\beta) + 2C\beta\delta,\\
(3)\quad & aC_1 = A\gamma^2 + B\gamma\delta + C\delta^2,
\end{aligned}\right\} \quad \alpha\delta - \beta\gamma = a.$$

Denn jedenfalls bestehen Gleichungen der Form (1), (2), (3), wo a eine Funktion ist. Setzt man andererseits $\omega_1 = \frac{\alpha\omega + \beta}{\gamma\omega + \delta}$ in $C_1\omega_1^2 + A_1 \quad B_1\omega_1$ ein, so erhält man Formeln, die aus (1), (2), (3) jedenfalls hervorgehen, indem A, B, C mit A_1, B_1, C_1 vertauscht werden, α durch δ, δ durch α ersetzt werden, und β, γ das Vorzeichen wechseln. Etwa:

$$\left.\begin{aligned}
& bA = A_1\delta^2 - B_1\beta\delta + C_1\beta^2,\\
& bB = -2A_1\gamma\delta + B_1(\alpha\delta + \beta\gamma) - 2C_1\alpha\beta,\\
& bC = A_1\gamma^2 - B_1\alpha\gamma + C_1\alpha^2,
\end{aligned}\right\} \quad \text{wo } b \text{ wieder eine ganze Funktion ist.}$$

Das Einsetzen in (1) ergibt nach Multiplikation mit b

$$abA_1 = A_1(\alpha\delta - \beta\gamma)^2, \quad \text{also} \quad ab = (\alpha\delta - \beta\gamma)^2,$$

so daß also a und b Einheiten sein müssen. (1) ergibt, wenn wir vorübergehend $\alpha\delta - \beta\gamma$ mit a' bezeichnen:

$$a'YC = aY_1C_1.$$

Da $\operatorname{sgn}(2YC) = \operatorname{sgn}(2Y_1C_1) = 1$ ist, haben wir $a' = a$, also auch $b = a$. Außer (1), (2), (3) gelten also die Formeln:

$$\left.\begin{aligned}
(4)\quad & 2YC = 2Y_1C_1,\\
(5)\quad & aA = A_1\delta^2 - B_1\delta\beta + C_1\beta^2,\\
(6)\quad & aB = -2A_1\gamma\delta + B_1(\alpha\delta + \beta\gamma) - 2C_1\alpha\beta,\\
(7)\quad & aC = A_1\gamma^2 - B_1\alpha\gamma + C_1\alpha^2,
\end{aligned}\right\} \quad \alpha\delta - \beta\gamma = a.$$

Sei nun D_1 die Diskriminante von $\omega_1 = X_1 + Y_1\sqrt{\ }$. Dann ist

$$D_1 = (2C_1Y_1)^2 A.$$

Also wegen (4)

$$D_1 = (2CY)^2 A = D = B^2 - 4AC = B_1^2 - 4A_1C_1,$$

somit:

Satz. Äquivalente Funktionen haben die gleiche Diskriminante.

§ 9.

Beziehung zwischen Funktionsklassen und Idealklassen — Identität der Klassenzahlen.

Wir betrachten jetzt nur Funktionen ω mit quadratfreier Diskriminante D und fassen zugleich den Körper $K(\sqrt{D})$ ins Auge.

Sei $\mathfrak{a}$ ein Ideal des Körpers mit der Basis

$$\omega_1 = 2CS, \quad \omega_2 = S(B + \sqrt{D}), \quad D = B^2 - 4AC.$$

Wir setzen

$$\omega = \frac{\omega_2}{\omega_1} = \frac{B+\sqrt{D}}{2C}.$$

Dann ist ω wegen $D = B^2 - 4AC$, da ja A, B, C keinen gemeinsamen Teiler haben, eine quadratische Irrationalität mit der Diskriminante D.

Jede andere Basis von $\mathfrak{a}$ hat die Form

$$\left.\begin{aligned}\omega_1^* &= \delta\omega_1 + \gamma\omega_2 \\ \omega_1^* &= \beta\omega_1 + \alpha\omega_2\end{aligned}\right\} \quad \text{mit} \quad \begin{vmatrix}\alpha & \beta \\ \gamma & \delta\end{vmatrix} = a,$$

wo α, β, γ, δ ganz rational sind, und umgekehrt ist jedes Funktionspaar dieser Form eine Basis von $\mathfrak{a}$. Wir bilden

$$\omega^* = \frac{\omega_2^*}{\omega_1^*} = \frac{\alpha\omega+\beta}{\gamma\omega+\delta},$$

so daß also $\omega^* \sim \omega$.

Ordnen wir also jedem Ideal seine Basisquotienten zu, so ist ersichtlich jedem Ideal genau eine Klasse äquivalenter Funktionen zugeordnet.

Sei nun $\mathfrak{b}$ ein mit $\mathfrak{a}$ äquivalentes Ideal: $\mathfrak{b} = \varrho\mathfrak{a}$. Wenn ω_1^*, ω_2^* eine Basis von $\mathfrak{a}$ ist, ist $\varrho\omega_1^*$, $\varrho\omega_2^*$ eine Basis von $\mathfrak{b}$, und umgekehrt.

Dem Ideal $\mathfrak{b}$ sind also zuzuordnen seine Basisquotienten $\frac{\varrho\omega_2^*}{\varrho\omega_1^*} = \frac{\omega_2^*}{\omega_1^*} \sim \omega$. Dem Ideal $\mathfrak{b}$ ist also genau die gleiche Funktionsklasse zugeordnet. Es kann ferner die Basis stets so gewählt werden, daß eine beliebige Funktion der Funktionsklasse entsteht.

Es möge nun umgekehrt $\mathfrak{a}$ und $\mathfrak{b}$ der gleichen Funktionsklasse zugeordnet sein. Wir wählen in $\mathfrak{a}$ und $\mathfrak{b}$ je eine Basis ω_1, ω_2 bzw. ω_1^*, ω_2^* derart, daß durch die Basisquotienten die gleiche Funktion entsteht; dies geht nach dem eben Gesagten. Es ist also $\frac{\omega_2}{\omega_1} = \frac{\omega_2^*}{\omega_1^*}$. Also gilt

$$\omega_1^* = \varrho\omega_1, \qquad \omega_2^* = \varrho\omega_2.$$

Dann ist ersichtlich $\mathfrak{b} = \varrho\mathfrak{a}$, da ϱ eine Funktion des Körpers ist.

Es ist also jeder Idealklasse genau eine Funktionsklasse zugeordnet und verschiedenen Idealklassen verschiedene Funktionsklassen.

Es entsteht aber auch jede Funktionsklasse der Diskriminante D. Denn gehört ihr etwa $\omega = \frac{B+\sqrt{D}}{2C}$ mit $D = B^2 - 4AC$ an, so ist $\omega_2 = B + \sqrt{D}$, $\omega_1 = 2C$ die Basis eines Ideals $\mathfrak{a}$, dem der Basisquotient $\frac{\omega_2}{\omega_1}$ zuzuordnen ist.

Es ist also eine ein-eindeutige Zuordnung zwischen den Idealklassen des Körpers $K(\sqrt{D})$ und den Funktionsklassen der Diskriminante D erreicht.

Ist also die Klassenzahl der Funktionsklassen der Diskriminante D endlich, so ist es auch die der Idealklassen, und ihre Anzahl stimmt überein.

Im weiteren Verlaufe wollen wir jedoch die Voraussetzung, daß D quadratfrei ist, wieder fallen lassen, da dadurch keine Vereinfachung erreicht wird.

Die Theorie der Einheiten werden wir auf dieser Grundlage gleichzeitig miterledigen.

Wir beginnen mit dem einfacheren Fall des imaginären Körpers.

§ 10.

Die Endlichkeit der Klassenzahl für imaginäre Funktionen.

Wir führen folgende Bezeichnung ein. Sei

$$X = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0 + a_{-1} t^{-1} + a_{-2} t^{-2} + \ldots$$

und $n \geqq 0$. Dann schreiben wir

$$E(X) = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_0.$$

Im Falle $n < 0$ dagegen sei

$$E(X) = 0.$$

Das Symbol $E(X)$ steht in Analogie zum Symbol „nächst kleinere ganze Zahl".

Definition. Die imaginäre quadratische Irrationalität $\omega = X + Y\sqrt{\Delta}$ heißt reduziert, wenn sie folgenden Bedingungen genügt:

$$|X| < 1, \tag{1}$$

$$|\omega\omega'| \geqq 1, \tag{2}$$

$$\operatorname{sgn} 2Y = 1. \tag{3}$$

Bedingung (2) ist wegen (1) vollkommen gleichbedeutend mit

$$|Y^2\Delta| \geqq 1. \tag{4}$$

Satz. Jede imaginäre quadratische Irrationalität $\omega = X + Y\sqrt{\Delta}$ ist äquivalent mit einer Reduzierten.

Beweis. Die Funktion $\bar{\omega} = \omega - E(X)$ genügt ersichtlich der Bedingung (1). Genügt sie der Bedingung (2) nicht, so setzen wir $\omega_1 = -\frac{1}{\bar{\omega}} = X_1 + Y_1\sqrt{\Delta}$, wo $\omega \sim \omega$, $\omega_1 \sim \omega$ ist, und bilden $\bar{\omega}_1 = \omega_1 - E(X_1)$. $\bar{\omega}_1$ genügt wieder (1). Genügt es (2) nicht, so sei wieder $\omega_2 = -\frac{1}{\bar{\omega}_1} = X_2 + Y_2\sqrt{\Delta}$ und $\bar{\omega}_2 = \omega_2 - E(X_2)$. So fahren wir fort.

Ich behaupte: Die Funktionen $\omega_\nu = \omega_\nu - E(X_\nu)$, wobei $\omega_\nu = -\frac{1}{\bar{\omega}_{\nu-1}}$ ist, welche alle der Bedingung (1) genügen und mit ω äquivalent sind, genügen schließlich der Bedingung (2).

Beweis. Wir setzen $R_\nu = \overline{\omega} \cdot \overline{\omega}'_\nu$ (R_ν ist also als Norm rational!). Dann ist

$$R_\nu = \left(-\frac{1}{\omega_{\nu+1}}\right)\left(-\frac{1}{\omega'_{\nu+1}}\right) = \frac{1}{\omega_{\nu+1}\,\omega'_{\nu+1}}, \quad \text{da ja} \quad \omega_{\nu+1} = -\frac{1}{\overline{\omega}_\nu}.$$

Also:

$$R_\nu = \frac{1}{X^2_{\nu+1} - Y^2_{\nu+1}\Delta} = \frac{1}{\omega_{\nu+1}\,\omega'_{\nu+1}}.$$

Aus $\overline{\omega}_\nu = -\frac{1}{\omega_{\nu+1}}$ folgt $\omega_\nu = E(X_\nu) - \frac{1}{\omega_{\nu+1}}$, also

$$X_\nu + Y_\nu\sqrt{\Delta} = E(X_\nu) - \frac{\omega'_{\nu+1}}{\omega_{\nu+1}\,\omega'_{\nu+1}} = E(X_\nu) - R_\nu \cdot \omega'_{\nu+1}.$$

Somit:

$$Y_\nu\sqrt{\Delta} = R_\nu\, Y_{\nu+1}\sqrt{\Delta}.$$

Wegen

$$Y_\nu\sqrt{\Delta} = \frac{\sqrt{D}}{2C_\nu},$$

falls $\omega_\nu = \{A_\nu, B_\nu, C_\nu\}$ gesetzt wird, und wobei $D = B_\nu^2 - 4A_\nu C_\nu$ ist (da ja äquivalente Funktionen gleiche Diskriminante haben), finden wir:

$$C_{\nu+1} = R_\nu C_\nu.$$

Solange nun $|R_\nu| < 1$ ist, finden wir

$$|C_{\nu+1}| < |C_\nu|.$$

Da es aber nur endlich viele ganze rationale Funktionen abnehmenden Grades geben kann, und $C_\nu \neq 0$ ist, muß schließlich einmal $|R_\nu| \geqq 1$ sein. Wegen $R_\nu = \overline{\omega}_\nu \overline{\omega}'_\nu$ bedeutet dies: $\overline{\omega}_\nu$ genügt der Bedingung (2). Setzt man nun

$$\overline{\omega}_\nu = \overline{X}_\nu + \overline{Y}_\nu\sqrt{\Delta},$$

so genügt die Funktion

$$\omega^* = \frac{\overline{\omega}_\nu}{2 \operatorname{sgn} \overline{Y}_\nu}$$

allen drei Bedingungen, und es ist $\omega^* \sim \omega$.

Die Reduziertenbedingung für die Funktion A, B, C finden wir, wenn wir in (1), (2), (4) einsetzen $X = \frac{B}{2C}$, $Y\sqrt{\Delta} = \frac{\sqrt{D}}{2C}$. Sie lauten:

$$|B| < |C| \leqq \sqrt{|D|} \quad \text{und} \quad \operatorname{sgn} C = 1.$$

Gleichzeitig muß $D = B^2 - 4AC$ sein, wegen $B^2| < |D|$ also $|AC| = |D|$ gelten.

Daraus folgt unmittelbar, daß es zu gegebener Diskriminante nur endlich viele reduzierte Funktionen geben kann, daß also die Klassenzahl von Funktionen gegebener Diskriminante endlich ist.

Für quadratische Körper, also quadratfreie Diskriminanten folgt speziell:

Satz. Die Anzahl der Idealklassen im imaginären Körper $K(\sqrt{D})$ ist endlich.

Wir fragen nun, wann zwei reduzierte Funktionen einander äquivalent sind.

Seien $\omega = \{A, B, C\}$ und $\omega_1 = \{A_1, B_1, C_1\}$ zwei äquivalente reduzierte Funktionen:

$$\omega_1 = \frac{\alpha\omega + \beta}{\gamma\omega + \delta}, \qquad \text{wo } \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = a.$$

Dann folgt aus § 8, (3):

$$4aCC_1 = (2C\delta + B\gamma)^2 - D\gamma^2.$$

Wenn nun der Betrag wenigstens einer der Funktionen C und C_1 kleiner ist als $\sqrt{|D|}$, also $|CC_1| < |D|$ ist, so folgt:

$$|(2C\delta + B\gamma)^2 - D\gamma^2| < |D|.$$

Wäre nun $\gamma \neq 0$, so könnten sich, da $\sqrt{D}$ imaginär ist, also D entweder ungeraden Grad hat oder $\operatorname{sgn} D = g$ ist, die höchsten Potenzen linker Hand nie heben, so daß der Betrag der linken Seite $\geqq |D|$ wäre. Also ist $\gamma = 0$. Dies hat $a = \alpha\delta$ zur Folge, so daß also α und δ triviale Einheiten sind. Aus § 8, (2), (3) folgt dann

$$aC_1 = C\delta^2, \qquad aB_1 = B\alpha\delta + 2C\beta\delta,$$

somit wegen $\operatorname{sgn} C = \operatorname{sgn} C_1 = 1$:

$$a = \alpha\delta = \delta^2, \quad \text{also} \quad \alpha = \delta.$$

Wäre nun $\beta \neq 0$, so erhielte man wegen $|B| < |C|$, da aus der ersten Gleichung $|C| = |C_1|$ folgt, $|B_1| \geqq |C| = |C_1|$, was nicht geht. Es ist also $\beta = \gamma = 0$; $\alpha = \delta$. Somit:

$$\omega_1 = \omega.$$

Ist nun der Grad von D ungerade, so ist stets $|C| < |\sqrt{D}|$. Dann sind also alle reduzierten Funktionen untereinander nicht äquivalent und ihre Anzahl die Klassenzahl.

Falls aber der Grad von D gerade ist, kann es reduzierte Funktionen mit $|C| = \sqrt{|D|}$ geben. Die Funktionen mit $|C| < \sqrt{|D|}$ sind dann sicher untereinander und zu denen mit $|C| = \sqrt{|D|}$ nicht äquivalent.

Es bleibt also nur noch der Fall

$$|C| = |C_1| = \sqrt{|D|},$$

zu erledigen. Wegen $|AC| = |D|$ ist dann

$$|A| = |A_1| = \sqrt{|D|}.$$

Nun leitet man aus § 8, (1), (3) folgende vier Formeln ab:

$$4aAA_1 = (2A\alpha + B\beta)^2 - D\beta^2,$$
$$4aCA_1 = (2C\beta + B\alpha)^2 - D\alpha^2,$$
$$4aAC_1 = (2A\gamma + B\delta)^2 - D\delta^2,$$
$$4aCC_1 = (2C\delta + B\gamma)^2 - D\gamma^2.$$

Die Beträge der linken Seiten sind genau $|D|$. Wenn nun eine einzige der Funktionen $\alpha, \beta, \gamma, \delta$ keine Zahl wäre, so würde dies in mindestens einer Formel auf einen Widerspruch führen. Wäre z. B. $\beta \leqq p$, so würden sich rechterhand in der ersten Formel die höchsten Potenzen nicht wegheben können, da ja $\sqrt{D}$ imaginär ist. Der Betrag der rechten Seite wäre also mindestens $|D\beta^2|$, entgegen dem Betrag der linken Seite.

Die Funktionen $\alpha, \beta, \gamma, \delta$ müssen also Zahlen sein.

Nun gehen wir aus von den Relationen § 8, (1), (2), (3), (6). Wir beachten:

$$C = |C_1| = |A| = |A_1| < \sqrt{|D|}, \qquad B < \sqrt{|D|},$$
$$|B_1| < \sqrt{|D|}, \quad \operatorname{sgn} C = \operatorname{sgn} C_1 = 1,$$

sowie:

$$\operatorname{sgn} D = g = \operatorname{sgn}(B^2 - 4AC) = \operatorname{sgn}(-4AC) = -4 \operatorname{sgn} A,$$

so daß also:

$$\operatorname{sgn} A = \operatorname{sgn} A_1 = -\frac{g}{4}$$

ist. Wir vergleichen nun die höchsten Koeffizienten rechts und links. In (2) und (6) müssen sich wegen $B < C$ die höchsten Koeffizienten rechts heben.

Wir erhalten so die Formeln

$$\left.\begin{aligned} -\tfrac{g}{4}a &= -\tfrac{g}{4}\alpha^2 + \beta^2 \\ 0 &= -\tfrac{g}{4}\alpha\gamma + \beta\delta \\ a &= -\tfrac{g}{4}\gamma^2 + \delta^2 \\ 0 &= -\tfrac{g}{4}\gamma\delta + \alpha\beta \end{aligned}\right\} \alpha\delta - \beta\gamma = a \neq 0.$$

Wenn umgekehrt

$$A| = |C| = \sqrt{|D|}, \qquad |B| < C, \qquad \operatorname{sgn} C = 1$$

und

$$\operatorname{sgn} A = -\frac{g}{4} \quad \text{mit} \quad D = B^2 - 4AC$$

ist, und die angeschriebenen Relationen erfüllt sind, so folgt aus (1), (2), (3), daß dann

$$|A_1| = |C_1| = \sqrt{|D|}, \quad |B_1| < \sqrt{|D|}, \quad \operatorname{sgn} C_1 = 1 \text{ und } \operatorname{sgn} A_1 = -\frac{g}{4}$$

ist. Daß also auch das transformierte ω_1 reduziert ist. Unsere Relationen sind also sowohl notwendig wie hinreichend.

1. $\alpha = 0$, also $-\beta\gamma = a$: $\beta \neq 0$, $\gamma \neq 0$; $\beta\delta = 0$, also $\delta = 0$. Ferner $a = -\beta\gamma = -\frac{g}{4}\gamma^2$; $\beta = \frac{g}{4}\gamma$. Also $\alpha = \delta = 0$, $\beta = \frac{g}{4}\gamma$, somit $\omega_1 = \frac{g}{4} \cdot \frac{1}{\omega}$.

2. $\delta = 0$, also $-\beta\gamma = a \neq 0$; $\alpha\beta = 0$, also $\alpha = 0$, d. h. Fall 1.

3. $\gamma = 0$, also $\alpha\delta = a \neq 0$; $\beta\delta = 0$; $\delta = 0$, $\alpha\delta = \delta^2$, somit $\alpha = \delta$, somit $\omega_1 = \omega$.

4. $\beta = 0$; $\alpha\delta = a \neq 0$; $\alpha\gamma = 0$, also $\gamma = 0$, also Fall 3.

Wenn also eine unserer Zahlen verschwindet, kann es sich nur entweder um die triviale Äquivalenzbeziehung $\omega = \omega_1$, oder um

$$\omega_1 = \frac{g}{4} \cdot \frac{1}{\omega}$$

handeln.

Unsere vier Zahlen seien also alle von Null verschieden. Aus $\frac{g}{4}\alpha\gamma = \beta\delta$ und $\frac{g}{4}\gamma\delta = \alpha\beta$ folgt durch Division $\alpha^2 = \delta^2$.

Wäre nun $\alpha = -\delta$, so hätte man $-\frac{g}{4}\gamma = \beta$. Also

$$a = \alpha\delta - \beta\gamma = -\delta^2 + \frac{g}{4}\gamma^2.$$

Da aber $a = \delta^2 - \frac{g}{4}\gamma^2$ ist, würde $a = -a$, also $a = 0$ folgen, was nicht geht.

Es ist also $\alpha = \delta$ und $\frac{g}{4}\gamma = \beta$. Dann sind aber auch alle unsere Relationen befriedigt und die zugehörige, mit ω äquivalente Funktion ω_1, da wie bereits gesagt, die Relationen notwendig und hinreichend sind, auch reduziert. Da noch eine unserer Zahlen beliebig wählbar ist, wählen wir $\gamma = 4$, so daß $\beta = g$ wird. Die Äquivalenzbeziehung lautet dann:

$$\omega_1 = \frac{\alpha\omega + g}{4\omega + \alpha} \qquad (\alpha = 1, 2, 3, \ldots, (p-1)).$$

Lassen wir auch noch $\alpha = 0$ zu, so kommen wir zur bereits gefundenen Äquivalenzbeziehung $\omega_1 = \frac{g}{4} \cdot \frac{1}{\omega}$.

Sei nun $D < -1$. (Der Fall $D = g$ soll gleich erledigt werden.)

Dann sind unsere äquivalenten Funktionen auch wirklich voneinander verschieden. Denn

$$\frac{\alpha\omega+g}{4\omega+\alpha}=\frac{\alpha_1\omega+g}{4\omega+\alpha_1}$$

hat zur Folge $(\alpha-\alpha_1)(4\omega^2-g)=0$.

Somit, wenn $\alpha \neq \alpha_1$ ist, $\omega=\frac{1}{2}\sqrt{g}$. Also der ausgeschlossene Fall $D=g$. Aus

$$\omega=\frac{\alpha\omega+g}{4\omega+\alpha}$$

folgt auch $4\omega^2=g$, also $D=g$.

Zusammenfassung. Für imaginäre quadratische Irrationalitäten sind die reduzierten Funktionen:

1. Im Falle ungeraden Grades von D nie untereinander äquivalent. Die Klassenzahl ist also gleich der Anzahl der reduzierten Funktionen.

2. Im Falle geraden Grades von D und $D \neq g$ sind die Funktionen mit $|C|<\sqrt{|D|}$ weder untereinander noch zu denen mit $|C|=\sqrt{|D|}$ äquivalent. Ihre Anzahl sei r.

Die Funktionen mit $|C|=\sqrt{|D|}$ zerfallen in Gruppen von je $(p+1)$ untereinander äquivalenten Funktionen. Ist ω eine Funktion dieser Gruppe, so sind die p übrigen gegeben durch

$$\omega_\alpha=\frac{\alpha\omega+g}{4\omega+\alpha} \qquad (\alpha=0,1,2,\ldots,p-1).$$

Funktionen aus verschiedenen Gruppen sind miteinander nicht äquivalent.

Ist s die Anzahl der reduzierten Funktionen mit $|C|=\sqrt{|D|}$, so ist s stets durch $p+1$ teilbar, und die Klassenzahl ist

$$h=r+\frac{s}{p+1}.$$

3. Im Falle $D=g$ muß $|C|\leqq 1$, also $C=1$ sein. Ferner $|B|<|C|$, also $B=0$. Dies liefert die einzige reduzierte Funktion $\omega=\frac{1}{2}\sqrt{g}$. Die Klassenzahl ist also eins.

Wenn D quadratfrei ist, ordnen wir den reduzierten Funktionen $\omega=\frac{B+\sqrt{D}}{2C}$ das Ideal $\mathfrak{a}$ von $K(\sqrt{D})$ mit der Basisdarstellung $\mathfrak{a}=(2C, B+\sqrt{D})$ zu. Dieses Ideal nennen wir ein „reduziertes Ideal“. Dann gibt es in jeder Idealklasse reduzierte Ideale. Für sie gilt, da $N\mathfrak{a}=C$ ist, $|N\mathfrak{a}|\leqq\sqrt{|D|}$.

Da die adaptierte Basis, wenn $\operatorname{sgn} C=1$ vorgeschrieben ist, durch das Ideal eindeutig bestimmt ist, sind verschiedenen reduzierten Funktionen verschiedene reduzierte Ideale zugeordnet. Nach dem Früheren entsprechen ferner äquivalenten Idealen äquivalente Funktionen und umgekehrt.

Beispiele. 1. $D = g$. Hier haben wir nur das reduzierte Ideal. $\mathfrak{a} = (2, \sqrt{g}) = (1)$. Die Klassenzahl ist also $h = 1$.

2. $D = t + a$. (Der Fall $D = gt + a$ ist nicht wesentlich verschieden.) Es muß $|C| \leqq 1$, also $C = 1$, $B = 0$ sein. Es gibt also nur die reduzierte Funktion $\omega = \frac{1}{2}\sqrt{t + a}$, im Körper nur das reduzierte Ideal $\mathfrak{a} = (2, \sqrt{D}) = (1)$. Wieder ist $h = 1$.

3. D sei quadratisch, $\operatorname{sgn} D = g$; also $|D| = p^2$, so daß $|C| \leqq p$ sein muß. Für $C = 1$, $B = 0$ liefert dies wieder $\omega = \frac{1}{2}\sqrt{D}$.

Hier haben wir aber noch das Vorkommen linearer C zu berücksichtigen. Zu diesem Zwecke denken wir uns in D durch passende Lineartransformation des Adjunktionsbuchstabens t (dies führt auf einen isomorphen Körper) den Koeffizienten von t zum Verschwinden gebracht. Dann kann über die Transformation noch so verfügt werden, daß nach Hinzufügung passend gewählter quadratischer Reste als Faktoren D eine der Formen

$$D = gt^2 - g, \qquad D = gt^2 - 1, \qquad D = gt^2$$

annimmt.

a) $D = g(t^2 - 1)$. Hier wähle man $C = t + 1$, $B = 0$ und erhält die reduzierte Funktion $\omega_1 = \frac{\sqrt{D}}{2(t+1)}$.

b) $D = g(t^2 - g^{-1})$. Es gibt nun sicher eine Zahl b so, daß $b^2 + 1$ Nichtrest wird. (Denn andernfalls gäbe es ja nur Reste.) Für dieses b ist $g^{-1}(b^2 + 1)$ sicher Rest, also $b^2 - D = -g[t^2 - g^{-1}(1 + b^2)]$ sicher keine Primfunktion. $b^2 - D$ hat also sicher einen Linearteiler $t + a$. Nun setzen wir $C = t - a$, $B = b$ und erhalten die reduzierte Funktion $\omega = \frac{b + \sqrt{D}}{2(t+a)}$.

c) $D = gt^2$. Hier ist $D - b^2 = g(t^2 - g^{-1}b^2)$ stets Primfunktion, wenn $b \neq 0$ ist. Nun muß aber, wenn C linear ist, B eine Zahl sein. Soll $D - b^2$ einen Linearteiler C haben, so muß also $B = b = 0$ sein und $C = t$, $A = -\frac{g}{4}t$. Dann ist aber A, B, C nicht teilerfremd. Also gibt es hier keine Reduzierten mit $|C| = p$. Doch kommt dieser Fall für Körper nicht in Betracht, da ja D durch ein Quadrat teilbar ist.

Wenn C linear ist, gibt es für B nur die Möglichkeiten $B = 0, 1, 2, \ldots, p - 1$. Zu jedem B kann es nun höchstens zwei reduzierte Funktionen geben, nämlich die eventuell linearen Teiler von $B^2 - D$. Im ganzen gibt es also höchstens $2p$ Funktionen unserer Art, somit, da ihre Anzahl durch $p + 1$ teilbar sein soll, entweder gar keine oder genau $p + 1$ äquivalente. In den beiden uns allein interessierenden Fällen a) b) tritt, da wir die Existenz einer Reduzierten unserer Art festgestellt haben, das letztere ein.

Wir haben also:

Ist D quadratfrei und quadratisch, so ist die Klassenzahl des imaginären Körpers $K(\sqrt{D})$ stets $h = 2$.

Dann gibt es zwei Arten reduzierter Ideale:

I. Das Hauptideal $\mathfrak{a} = (2, \sqrt{D}) = (1)$.

II. Nichthauptideale der Form $\mathfrak{a} = (t + a, b + \sqrt{D})$, wo $t - a$ ein Teiler von $b^2 - D$ ist (a, b Zahlen). Und zwar gibt es genau $p - 1$ verschiedene miteinander äquivalente.

§ 11.

Die Anzahl der ambigen Klassen.

Satz. Enthält eine ambige Klasse ein ambiges Ideal, so enthält sie auch ein ambiges reduziertes Ideal.

Beweis. Die Klasse $\mathfrak{K}$ enthalte das ambige Ideal $\mathfrak{a}$ mit der Basisdarstellung $\mathfrak{a} = (2CS, (B + \sqrt{D})S) = (S) \cdot (2C, B + \sqrt{D})$. Da $\mathfrak{a}' = (S)(2C, B - \sqrt{D})$ ist, muß $(2C, B - \sqrt{D}) = (2C, B + \sqrt{D})$ sein (da ja $\mathfrak{a} = \mathfrak{a}'$ ist). Nun ist $\mathfrak{a} \sim (2C, B + \sqrt{D})$, so daß wir vom ambigen Ideal $\mathfrak{a} = (2C, B + \sqrt{D})$ ausgehen. In ihm können wir annehmen, es sei $\operatorname{sgn} C = 1$. Dann ist die adaptierte Basis eindeutig bestimmt. Da $\mathfrak{a}' = (2C, B - \sqrt{D}) = (2C, -B + \sqrt{D}) = \mathfrak{a}$ ist, muß also $B = -B$, also $B = 0$ sein. Wegen $D = -4AC$ ist also C ein Teiler von D. (Es wurde natürlich stillschweigend $|B| < |C|$ vorausgesetzt, was wir annehmen dürfen. Denn nur dann ist die adaptierte Basis eindeutig.) Es ist also $\mathfrak{a} = (2C, \sqrt{D})$. Setzen wir $D = CC' \operatorname{sgn} D$, so ist $\operatorname{sgn} C' = 1$ und C und C' relativ prim. Demnach, wenn $\mathfrak{b} = (2C', \sqrt{D})$ gesetzt wird:

$$\mathfrak{a} \cdot \mathfrak{b} = (2C, \sqrt{D})(2C', \sqrt{D}) = (4CC', 2C'\sqrt{D}, 2C\sqrt{D}, D)$$

$$= (D, \sqrt{D}) = (\sqrt{D}).$$

Also ist $\mathfrak{a}\mathfrak{b} = (\sqrt{D})$, somit, wegen $\mathfrak{a} = \mathfrak{a}'$:

$$(N\mathfrak{a}) \cdot \mathfrak{b} = (\sqrt{D})\mathfrak{a} \quad \text{oder} \quad \mathfrak{b} \sim \mathfrak{a}.$$

Ist also $|C| \geqq \sqrt{|D|}$, so ist $|C'| \leqq \sqrt{|D|}$. Eines der Ideale $\mathfrak{a}$ und $\mathfrak{b}$ ist also reduziert. Da $\mathfrak{a} \sim \mathfrak{b}$ ist, gibt es also in $\mathfrak{K}$ ein ambiges reduziertes Ideal, dessen Basisdarstellung dann lautet:

$$\mathfrak{a} = (2C, \sqrt{D}) \quad \text{mit} \quad |C| \leqq \sqrt{|D|}, \quad \text{wo } C \text{ ein Teiler von } D.$$

Durchläuft C diese Teiler, so erhält man alle ambigen reduzierten Ideale. Die mit $|C| < \sqrt{|D|}$ sind nach unseren Ergebnissen sicher untereinander und mit denen mit $|C| = \sqrt{|D|}$ nicht äquivalent. Zwei verschiedene Ideale $\mathfrak{a} = (2C, \sqrt{D})$, $\mathfrak{b} = (2C', \sqrt{D})$, wo C und C' zwei

Funktionen des Betrags $\sqrt{|D|}$ sind und zu den Teilern von D gehören, sind nach dem Früheren dann und nur dann äquivalent, wenn die zugeordneten Funktionen $\omega = \frac{\sqrt{D}}{2C}$, $\omega_1 = \frac{\sqrt{D}}{2C'}$ es sind. Ferner muß die Äquivalenzbeziehung die Form haben

$$\omega_1 = \frac{\alpha\omega + g}{4\omega + \alpha} \qquad (\alpha = 0, 1, 2, \ldots, p-1).$$

Dies liefert

$$\frac{D}{CC'} + \alpha\frac{\sqrt{D}}{2C'} = \alpha\frac{\sqrt{D}}{2C} + g.$$

Somit

$$D = gCC', \qquad \alpha = 0.$$

Es sind also genau zwei reduzierte Ideale einander äquivalent.

Die Anzahl der einander nicht äquivalenten reduzierten Ideale ist also genau die halbe Teilerzahl von D. Denn ist C ein Teiler, und setzen wir $D = CC'\,\mathrm{sgn}\,D$, so ist jedem Teiler C mit $|C| < \sqrt{|D|}$ ein anderer mit $|C| > \sqrt{|D|}$ zugeordnet. Die Teiler mit $|C| = \sqrt{D}$ liefern aber nur halb so viel Klassen, wie eben gezeigt wurde.

Wenn also:

$D = g^r P_1 P_2 \ldots P_s$ die Zerlegung von D in Primfunktionen ist, so ist die Anzahl der ambigen Idealklassen, welche ambige Ideale enthalten, genau 2^{s-1}.

Sei nun $\mathfrak{K}$ eine ambige Idealklasse ohne ambiges Ideal und $\mathfrak{a}$ ein reduziertes Ideal der Basisdarstellung $\mathfrak{a} = (2C, B + \sqrt{D})$. Dann ist $B \neq 0$, da sonst $\mathfrak{a}$ ambig wäre. Es ist also, da die Basisdarstellung eindeutig ist, $\mathfrak{a}' = (2C, -B + \sqrt{D})$ ein von $\mathfrak{a}$ verschiedenes und zwar ersichtlich gleichfalls reduziertes Ideal. Nun soll $\mathfrak{a} \sim \mathfrak{a}'$ sein. Dies geht nur, wenn $|C| = \sqrt{|D|}$ (nach dem vorigen Paragraphen) und somit der Grad von D gerade ist. Ist der Grad von D ungerade, so gibt es also keine ambigen Klassen ohne ambiges Ideal.

Wenn nun D geraden Grad hat, seien $\omega = \frac{B + \sqrt{D}}{2C}$, $\omega_1 = \frac{-B + \sqrt{D}}{2C}$ die beiden $\mathfrak{a}$ und $\mathfrak{a}'$ zugeordneten Funktionen.

Damit die Klasse $\mathfrak{K}$ ambig ohne ambiges Ideal sei, ist folgendes notwendig und hinreichend:

1. Es muß sein $\mathfrak{a} \sim \mathfrak{a}'$, also $\omega \sim \omega_1$, somit

$$\omega_1 = \frac{\alpha\omega + g}{4\omega + \alpha} \qquad (\alpha = 0, 1, 2, \ldots, p-1),$$

was

$$4\omega\omega_1 + \alpha(\omega_1 - \omega) = g$$

liefert, und schließlich

$$4A + \alpha B + gC = 0,$$

wo $|A| = |C| = \sqrt{|D|}$ und $|B| < |C|$.

2. Es darf die Idealklasse kein ambiges Ideal, also, da jede Klasse mit ambigem Ideal ein ambiges reduziertes enthält, kein ambiges reduziertes Ideal enthalten, dessen Basis $(2C_1, \sqrt{D})$ lautet. Mit ω sind aber äquivalent nur die Reduzierten

$$\frac{\beta\omega + g}{4\omega + \beta} \qquad (\beta = 0, 1, 2, \ldots, p-1),$$

wo sich dann die Funktionen A, B, C nach § 8, (1), (2), (3) transformieren. Dafür ist notwendig und hinreichend, daß in § 8, (2) das transformierte B_1 für alle β von 0 verschieden ist, daß also

$$aB_1 = 8A\beta + B(\beta^2 + 4g) + 2Cg\beta \not\equiv 0.$$

3. Muß $D \equiv B^2 - 4AC$ sein.

Gibt es andrerseits drei Funktionen A, B, C mit $\operatorname{sgn} C = 1$, welche 1. 2. 3. befriedigen, so bilden sie ein Ideal, welches einer ambigen Idealklasse ohne ambiges Ideal angehört. In

$$8A\beta + B(\beta^2 + 4g) + 2Cg\beta \not\equiv 0 \quad \text{für alle } \beta$$

setzen wir nun ein $4A = -\alpha B - gC$ und erhalten

$$B(\beta^2 - 2\alpha\beta + 4g) \not\equiv 0$$

oder, da $B \not\equiv 0$ ist,

$$\beta^2 - 2\alpha\beta + 4g \not\equiv 0$$

oder endlich

$$(\beta - \alpha)^2 \not\equiv \alpha^2 - 4g.$$

Dies muß für jedes β gelten. Dann kann also links jeder Rest stehen, wie auch α gewählt sei. Damit die Relation befriedigt wird, muß also $\alpha^2 - 4g$ Nichtrest werden.

Für wenigstens eines dieser α soll also

$$4A = -\alpha B - gC$$

zugleich mit

$$D = B^2 - 4AC$$

bestehen. Also muß

$$D = B^2 + \alpha BC + gC^2$$

sein oder

$$4gD = (2gC + \alpha B)^2 - (\alpha^2 - 4g) \cdot B^2.$$

Setzt man $D = gD_1$, so wird also die notwendige und hinreichende Bedingung dafür, daß es eine ambige Idealklasse ohne ambiges Ideal gibt, an die Existenz einer Zahl α geknüpft, für die $(\alpha^2 - 4g)$ Nichtrest wird und

$$D_1 = \left(C + \frac{\alpha}{2g}B\right)^2 - (\alpha^2 - 4g)\left(\frac{B}{2g}\right)^2$$

wird.

Wegen $C \sim B$ zeigt eine leichte Überlegung, daß dazu notwendig und hinreichend ist, daß D_1 eine Darstellung in der Form

$$D_1 = X^2 - gY^2 \quad \text{mit} \quad |X| > |Y|$$

gestattet. a kann dabei sogar beliebig gewählt werden, nur muß $a^2 - 4g$ Nichtrest werden, was stets geht.

Diese letzte Bedingung ist aber vollständig äquivalent mit der, daß es überhaupt eine Darstellung der Form

$$D_1 = c(X^2 - gY^2)$$

gibt, wo c irgendeine rationale Einheit ist. Denn aus ihr erhalten wir sofort die neuen Darstellungen

$$D_1 = \frac{c}{a^2 - b^2 g}(a^2 - b^2 g)(X^2 - gY^2) = \frac{c}{a^2 - b^2 g}(X_1^2 - gY_1^2),$$

wo

$$X_1 = aX + bgY, \qquad Y_1 = aY + bX$$

ist und a, b irgendwelche nicht gleichzeitig verschwindende Zahlen sind.

Wenn nun $|X| \neq |Y|$ ist, so wird, wenn $a \neq 0$, $b \neq 0$ gewählt wird, eine Darstellung mit $|X_1| = |Y_1|$ erhalten. Wir können also voraussetzen, es sei $|X| = |Y|$.

Da sich dann des Faktors g wegen die höchsten Potenzen sicher nicht wegheben, muß $|D| = |X^2| = |Y^2|$ sein, was wegen $\operatorname{sgn} D_1 = 1$ zu der Relation führt

$$1 = c((\operatorname{sgn} X)^2 - g(\operatorname{sgn} Y)^2).$$

Nun setzen wir $a = c \operatorname{sgn} X$, $b = -c \operatorname{sgn} Y$. Dann heben sich sicher in Y_1 rechterhand die höchsten Potenzen, in X_1 aber nicht, so daß $|X_1| > |Y_1|$ wird. Ferner ist

$$a^2 - b^2 g = c^2((\operatorname{sgn} X)^2 - g(\operatorname{sgn} Y)^2) = c.$$

Wir haben also wirklich eine Darstellung

$$D_1 = X_1^2 - gY_1^2 \quad \text{mit} \quad |X_1| > |Y_1|$$

erhalten.

Da wir nun in § 15 sehen werden, daß D_1 dann und nur dann eine Darstellung der Form $D_1 = c(X^2 - gY^2)$ gestattet, wenn es durch keine Primfunktion ungeraden Grades teilbar ist, so können wir, wenn wir dies hier vorwegnehmen wollen, unser Ergebnis so aussprechen (ist D von ungeradem Grade, so ist es ja sicher durch eine Primfunktion ungeraden Grades teilbar):

Im imaginären Körper $K(\sqrt{D})$ existiert dann und nur dann eine ambige Idealklasse, welche kein ambiges Ideal enthält, wenn D durch keine Primfunktion ungeraden Grades teilbar ist.

Unsere Entwicklungen gestatten auch die Repräsentanten dieser Klassen zu berechnen.

Hilfssatz. Sei $K(\sqrt{D})$ ein beliebiger Körper (imaginär oder reell), α eine ganze oder gebrochene Funktion des Körpers, für welche $N(\alpha) = +1$ ist. Dann gibt es eine ganze Funktion β des Körpers, so daß

$$\alpha = \frac{\beta}{\beta'}$$

wird.

Beweis. Sei $N(\alpha) = \alpha\alpha' = +1$. Wir wählen A ganz rational so, daß $\beta = A(1 + \alpha)$ ganz wird. Dann ist $\beta' = A(1 + \alpha')$ und somit

$$\frac{\beta}{\beta'} = \frac{1+\alpha}{1+\alpha'} = \frac{\alpha(1+\alpha)}{\alpha+\alpha\alpha'} = \frac{\alpha(1+\alpha)}{\alpha+1} = \alpha.$$

Sei jetzt $\mathfrak{K}$ eine beliebige ambige Idealklasse ohne ambiges Ideal und $\mathfrak{a}$ ein Ideal aus $\mathfrak{K}$. Da $\mathfrak{a} \sim \mathfrak{a}'$ ist, können wir setzen $\frac{\mathfrak{a}}{\mathfrak{a}'} = \alpha$, wo α eine bis auf eine Körpereinheit feste, ganze oder gebrochene Funktion ist. Durch Normenbildung geht hervor, daß $N(\alpha) = a$ ist, wo a eine rationale Einheit ist. Durch Hinzufügung einer passenden rationalen Einheit zu α kann erreicht werden, daß $N(\alpha) = 1$ oder $N(\alpha) = g$ wird. Aus $N(\alpha) = 1$ würde folgen, daß ein ganzes β existiert, so daß $\alpha = \frac{\beta'}{\beta}$ ist. Dann wäre $(\beta\mathfrak{a}) = (\beta\mathfrak{a})'$, also $\beta\mathfrak{a}$ ein ambiges Ideal. Da aber nun $\mathfrak{a} \sim \beta\mathfrak{a}$ ist, kann dies nicht zutreffen, da $\mathfrak{K}$ kein ambiges Ideal enthält. Es ist also $N(\alpha) = g$.

Sei jetzt $\mathfrak{K}_1$ eine zweite ambige Klasse ohne ambiges Ideal, der das Ideal $\mathfrak{a}_1$ angehört. Wieder ist:

$$\frac{\mathfrak{a}_1}{\mathfrak{a}_1'} = \alpha_1 \quad \text{mit} \quad N(\alpha_1) = g$$

und somit

$$\frac{\mathfrak{a}\,\mathfrak{a}_1'}{\mathfrak{a}'\mathfrak{a}_1} = \frac{(\mathfrak{a}\,\mathfrak{a}_1')}{(\mathfrak{a}\,\mathfrak{a}_1')'} = \frac{\alpha}{\alpha_1}, \quad \text{wo jetzt} \quad N\left(\frac{\alpha}{\alpha_1}\right) = 1$$

ist. Es gibt also eine ganze Funktion β, so daß $\frac{\alpha}{\alpha_1} = \frac{\beta}{\beta'}$ ist. Also ist

$$\frac{\mathfrak{a}\,\mathfrak{a}_1'}{(\mathfrak{a}\,\mathfrak{a}_1')'} = \frac{\beta}{\beta'}, \quad \text{oder} \quad \mathfrak{a}\,\mathfrak{a}_1'\beta' = (\mathfrak{a}\,\mathfrak{a}_1'\beta')'.$$

Da nun $\mathfrak{a}_1' \sim \mathfrak{a}_1$ also $\mathfrak{a}\,\mathfrak{a}_1'\beta' \sim \mathfrak{a}\,\mathfrak{a}_1$ und somit $\mathfrak{a}\,\mathfrak{a}_1'\beta'$ ein Ideal aus $\mathfrak{K}\,\mathfrak{K}_1$ ist, enthält die Klasse $\mathfrak{K}\,\mathfrak{K}_1$ ein ambiges Ideal und ist also eine Klasse $\mathfrak{K}_2$ mit ambigen Idealen.

Aus $\mathfrak{K}\,\mathfrak{K}_1 = \mathfrak{K}_2$ folgt aber wegen $\mathfrak{K}^2 = \mathfrak{K}_0$ Hauptklasse: $\mathfrak{K}_1 = \mathfrak{K}\,\mathfrak{K}_2$, wo $\mathfrak{K}_2$ ambig und mit ambigem Ideal ist.

Ist andrerseits $\mathfrak{K}$ ambig ohne ambiges Ideal, $\mathfrak{K}_2$ ambig mit ambigem Ideal, so wegen $\mathfrak{K}' = \mathfrak{K}$, $\mathfrak{K}_2' = \mathfrak{K}_2$ auch $(\mathfrak{K}\,\mathfrak{K}_2)' = \mathfrak{K}\,\mathfrak{K}_2$, also $\mathfrak{K}\,\mathfrak{K}_2$ ambig.

Enthielte $\mathfrak{K}\mathfrak{K}_2$ ein ambiges Ideal $\mathfrak{a}_1$, so wäre, $\mathfrak{K}\mathfrak{K}_2 = \mathfrak{K}_1$ gesetzt, $\mathfrak{K} = \mathfrak{K}_1\mathfrak{K}_2$. Ist nun $\mathfrak{a}_2$ ein ambiges Ideal von $\mathfrak{K}_2$, so ist $\mathfrak{a}_1\mathfrak{a}_2$ ein ambiges Ideal aus $\mathfrak{K}$. Es muß also $\mathfrak{K}_1 = \mathfrak{K}\mathfrak{K}_2$ ambig ohne ambiges Ideal sein. Aus der Gruppeneigenschaft erhellt noch, daß lauter verschiedene Klassen erhalten werden, wenn in $\mathfrak{K}\mathfrak{K}_2$ der zweite Faktor alle ambigen Klassen mit ambigem Ideal durchläuft.

Alle ambigen Klassen ohne ambiges Ideal erhält man also aus einer von ihnen etwa $\mathfrak{K}$ durch Bildung von $\mathfrak{K}\mathfrak{K}_2$, wo $\mathfrak{K}_2$ alle ambigen Klassen mit ambigem Ideal durchläuft.

Entweder gibt es also überhaupt keine ambigen Klassen ohne ambiges Ideal, oder ihre Anzahl ist genau so groß wie die der Klassen, welche ambige Ideale enthalten.

Daraus folgt:

Satz. Wenn $D = a \cdot P_1 P_2 P_3 \dots P_s$ die Zerlegung von D in Primfunktionen ist, so ist die Anzahl der ambigen Klassen des imaginären Körpers $K(\sqrt{D})$ gleich

$$2^{s-1} \quad \text{oder} \quad 2^s,$$

je nachdem D durch eine Primfunktion ungeraden Grades teilbar ist oder nicht.

Dies ist dann für die Gruppe der Idealklassen die Anzahl der Geschlechter. Für die Klassenzahl gilt in den beiden Fällen die Zerlegung

$$h = 2^{s-1} \cdot f \quad \text{bzw.} \quad h = 2^s \cdot f,$$

wo f ganz ist.

Ungerade kann also die Klassenzahl nur sein, wenn D eine Primfunktion ungeraden Grades ist.

§ 12.

Kettenbrüche.

Sei F eine reelle Funktion, $E(F)$ das in § 10 definierte Symbol.

Definition. Unter der Kettenbruchentwicklung einer Funktion F verstehen wir folgenden Algorithmus:

Wir setzen sukzessive

$$F = E(F) + \frac{1}{F_1}$$

$$F_1 = E(F_1) + \frac{1}{F_2}$$

$$F_2 = E(F_2) + \frac{1}{F_3}$$

$$\dots\dots\dots\dots$$

Dabei soll der Prozeß abbrechen, wenn einmal F_ν ganz ist, also

$$F_\nu = E(F_\nu)$$

wird. Anderenfalls werde er beliebig weit fortgesetzt.

Aus

$$F_{\nu-1} = E(F_{\nu-1}) + \frac{1}{F_\nu}$$

folgt für $\nu \geqq 1$ wegen der Bedeutung des Symbols $E(F)$, daß

$$\left|\frac{1}{F_\nu}\right| \leqq p^{-1}, \quad \text{also} \quad |F_\nu| \geqq p,$$

und demnach auch

$$|E(F_\nu)| \geqq p.$$

Bricht die Entwicklung mit F_n ab, ist also $F_n = E(F_n)$, so erkennen wir sukzessive: F_n ist rational, also auch F_{n-1}, usw. Es ist also F rational.

Sei umgekehrt F rational: $F = \frac{R}{R_0}$, wo R und R_0 ganz rational sind. Der Algorithmus ergibt:

$$\begin{aligned}
F &= E\left(\frac{R}{R_0}\right) + \frac{R_1}{R_0}, && |R_1| < |R_0|,\\
\frac{R_0}{R_1} &= E\left(\frac{R_0}{R_1}\right) + \frac{R_2}{R_1}, && |R_2| < |R_1|,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\frac{R_{\nu-1}}{R_\nu} &= E\left(\frac{R_{\nu-1}}{R_\nu}\right) + \frac{R_{\nu+1}}{R_\nu}, && |R_{\nu+1}| < |R_\nu|.
\end{aligned}$$

Da die Grade stets abnehmen, und unsere Funktionen ganz rational sind, muß schließlich einmal $R_{\nu+1} = 0$ sein, also unser Prozeß abbrechen.

Die Kettenbruchentwicklung bricht also dann und nur dann nie ab, wenn F irrational ist.

Wir wollen nun weiterhin F als irrational voraussetzen. Im Algorithmus $F_\nu = E(F_\nu) + \frac{1}{F_{\nu+1}}$ setzen wir zur Abkürzung $E(F_\nu) = A_\nu$. Dann ist also

$$|A_\nu| \geqq p \quad \text{für} \quad \nu \geqq 1,$$

und es ist

$$F = A_0 + \frac{1}{A_1} + \frac{1}{A_2} + \cdots + \frac{1}{A_{n-1}} + \frac{1}{F_n}.$$

Die Funktion F_n werde Schlußfunktion genannt. Wie beim gewöhnlichen Kettenbruch gilt die Formel

$$F = \frac{P_n F_n + P_{n-1}}{Q_n F_n + Q_{n-1}},$$

wobei P_n und Q_n ganz rational sind und nach den Rekursionen

$$\left.\begin{aligned} P_{n+1} &= P_n A_n + P_{n-1} \\ Q_{n+1} &= Q_n A_n + Q_{n-1} \end{aligned}\right\} \text{ mit } \left\{\begin{aligned} P_0 &= 1; \quad P_1 = A_0 \\ Q_0 &= 0; \quad Q_1 = 1 \end{aligned}\right.$$

berechnet werden. Es ist daher

$$\begin{aligned} Q_2 &= A_1, && \text{also} \quad |Q_2| = |Q_1 A_1| \geqq p, \\ Q_3 &= Q_2 A_2 + 1, && \text{also} \quad |Q_3| = |Q_2 A_2| > |Q_2|, \\ Q_4 &= Q_3 A_3 + Q_2, && \text{also} \quad |Q_4| = |Q_3 A_3| > |Q_2|, \end{aligned}$$

somit durch Induktion:

$$|Q_\nu| = |Q_{\nu-1} A_{\nu-1}|, \quad \text{also} \quad |Q_\nu| = |A_{\nu-1} A_{\nu-2} \dots A_1|.$$

Wegen $|A_\nu| \geqq p$ für $\nu \geqq 1$ finden wir

$$|Q_\nu| \geqq p^{\nu-1} \quad \text{für} \quad \nu \geqq 1.$$

Ferner liefert das Rekursionssystem:

$$P_n Q_{n-1} - Q_n P_{n-1} = (-1)^n.$$

Dies zeigt, daß P_n und Q_n prim sind.

Satz. Bei einem unendlichen Kettenbruch ist die Folge der Näherungsbrüche: $\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \dots$ konvergent und es ist:

$$\lim_{\nu=\infty} \frac{P_\nu}{Q_\nu} = F.$$

Beweis. Aus

$$F = \frac{P_\nu F_\nu + P_{\nu-1}}{Q_\nu F_\nu + Q_{\nu-1}}$$

folgt

$$F - \frac{P_\nu}{Q_\nu} = \frac{P_{\nu-1} Q_\nu - P_\nu Q_{\nu-1}}{Q_\nu (Q_\nu F_\nu + Q_{\nu-1})} = \frac{(-1)^{\nu-1}}{Q_\nu (Q_\nu F_\nu + Q_{\nu-1})}.$$

Für $\nu \geqq 1$ ist aber $F_\nu = A_\nu + R_\nu$, also, da $|R_\nu| \leqq p^{-1}$ ist,

$$|Q_\nu F_\nu + Q_{\nu-1}| = |Q_\nu A_\nu + Q_{\nu+1}|.$$

Also

$$\left|F - \frac{P_\nu}{Q_\nu}\right| = \frac{1}{|Q_\nu Q_{\nu+1}|} \leqq p^{-(2\nu-1)}.$$

Daraus geht unsere Behauptung unmittelbar hervor.

§ 13.

Kettenbruchentwicklung quadratischer Irrationalitäten — Endlichkeit der Klassenzahl.

Definition. Eine reelle quadratische Irrationalität ω heißt reduziert, wenn ihr Betrag größer als eins, der ihrer Konjugierten aber kleiner als eins ist:

$$|\omega'| < 1 < |\omega|.$$

Satz. Jede reelle quadratische Irrationalität ω ist äquivalent mit einer Reduzierten.

Beweis. Wir entwickeln ω in einen Kettenbruch, dessen Schlußzahlen ω_ν seien. Da ω_ν Schlußfunktion ist, gilt

$$\omega_\nu > 1.$$

Ferner ist

$$\omega = \frac{P_\nu \omega_\nu + P_{\nu-1}}{Q_\nu \omega_\nu + Q_{\nu-1}} \quad \text{mit} \quad \begin{vmatrix} P_\nu & P_{\nu-1} \\ Q_\nu & Q_{\nu-1} \end{vmatrix} = (-1)^\nu,$$

so daß $\omega \sim \omega_\nu$.

Durch Auflösung erhält man

$$\omega_\nu = -\frac{Q_{\nu-1}\omega - P_{\nu-1}}{Q_\nu \omega - P_\nu},$$

also

$$|1| \qquad \omega_\nu' = -\frac{Q_{\nu-1}\omega' - P_{\nu-1}}{Q_\nu \omega' - P_\nu} = \frac{Q_{\nu-1}}{Q_\nu} \cdot \frac{\omega' - \omega) + \left(\omega - \frac{P_{\nu-1}}{Q_{\nu-1}}\right)}{(\omega' - \omega) + \left(\omega - \frac{P_\nu}{Q_\nu}\right)}.$$

Setzen wir nun $\omega' - \omega = p^r$, so gilt sicher für $\nu \geqq r - 2$

$$\omega - \frac{P_{\nu-1}}{Q_{\nu-1}} \leqq p^{-(2\nu-3)} \leqq p^{-(2|r|+1)},$$

$$\omega - \frac{P_\nu}{Q_\nu} \Big| \leqq p^{-(2\nu-1)} \leqq p^{-(2|r|+3)},$$

so daß im zweiten Bruch rechterhand $|1|$ Zähler und Nenner den gleichen Betrag haben. Für $\nu \geqq |r| + 2$ gilt also

$$\omega_\nu' = \frac{Q_{\nu-1}}{Q_\nu} = \frac{1}{A_{\nu-1}} \leqq p^{-1} < 1.$$

was mit $\omega_\nu > 1$ zusammen die Reduziertenbedingung ausmacht.

Satz. Ist ω reduziert, und setzen wir $\omega - E(\omega) = \frac{1}{\omega_1}$, so ist auch ω_1 reduziert. Wegen $\omega_1 \sim \omega$ hat ω_1 die gleiche Diskriminante wie ω.

Beweis. Wegen $\omega - E(\omega) < 1$ gilt $|\omega_1| > 1$. Da nun $\omega > 1$ ist, ist auch $E(\omega) > 1$. Wegen $|\omega'| < 1$ ist also

$$\omega' - E(\omega) = -E(\omega) > 1,$$

somit

$$\omega_1' = -\frac{1}{\omega' - E(\omega)} < 1.$$

Also ist ω_1 auch reduziert.

Satz. In der Beziehung $\omega - E(\omega) = \frac{1}{\omega_1}$ seien ω und ω_1 reduziert. Dann ist nach Vorgabe von ω_1 bereits ω eindeutig bestimmt.

Beweis. Wir haben $\omega' - E(\omega) = -\frac{1}{\omega_1'}$, wo $\omega' < 1$ und $\left|\frac{1}{\omega_1'}\right| > 1$ ist.

Also ist

$$E(\omega) = -E\left(\frac{1}{\omega_1'}\right),$$

somit

$$\omega = -E\left(\frac{1}{\omega_1'}\right) + \frac{1}{\omega_1},$$

womit ω bestimmt ist.

Daraus folgt: Die Schlußfunktionen ω_ν in der Kettenbruchentwicklung einer reellen quadratischen Irrationalität ω sind schließlich reduziert, und mit einer von ihnen sind es auch alle folgenden.

Ist speziell ω reduziert, so sind alle Schlußfunktionen reduziert, und mit einer von ihnen sind nicht nur alle folgenden, sondern auch alle vorhergehenden eindeutig bestimmt.

Für die Funktionen A, B, C lautet wegen

$$\omega = \frac{B+\sqrt{D}}{2C}, \quad \omega' = \frac{B-\sqrt{D}}{2C}$$

die Reduziertenbedingung

$$|B-\sqrt{D}| < |C| < |B+\sqrt{D}|.$$

Wäre nun $|B| \neq |\sqrt{D}|$, so wäre $|B+\sqrt{D}| = |B-\sqrt{D}|$, so daß die Ungleichheitszeichen nicht stehen könnten. Es ist also $|B| = |\sqrt{D}|$. Ferner müssen, da ja beide Ungleichheitszeichen gelten sollen, die Grade von $B-\sqrt{D}$ und $B+\sqrt{D}$ sich also um mindestens zwei Einheiten unterscheiden müssen, die beiden höchsten Potenzen von B und $\sqrt{D}$ übereinstimmen. Dies gibt nur endlich viel Möglichkeiten für B, falls D vorgegeben ist, und unserer Ungleichung halber zu jedem B nur endlich viele C, die noch durch die Bedingung $D = B^2 - 4AC$ eingeschränkt werden.

Es gibt also zu gegebener Diskriminante D nur endlich viele Reduzierte, also ist die Klassenanzahl der Funktionen der Diskriminante D endlich.

Wenn D quadratfrei ist, folgt speziell:

Satz. Im reellen quadratischen Körper $K(\sqrt{D})$ ist die Anzahl der Idealklassen endlich.

Ferner allgemein:

Die Kettenbruchentwicklung einer reduzierten quadratischen Irrationalität und nur einer solchen, ist rein periodisch. Die der übrigen (quadratischen) Irrationalitäten gemischt periodisch.

Beispiel. Der einfachste reelle Körper ist $K(\sqrt{t^2+a_1 t+a_2})$, wo $a_2 - \frac{1}{4}a_1^2 \neq 0$ sein muß, da sonst D ein volles Quadrat ist. Wir haben $\sqrt{D} = t + \frac{1}{2}a_1 + \ldots$. Da die beiden ersten Potenzen von B und $\sqrt{D}$

übereinstimmen, ist $B = t + \frac{1}{2}a_1$, also $D - B^2 = a_2 - \frac{1}{4}a_1^2 \neq 0$. Also muß C eine Einheit b sein. Die reduzierten Funktionen sind also: $c(t + \frac{1}{2}a_1 + \sqrt{D})$. Sie sind miteinander äquivalent, also ist die Klassenzahl unseres Körpers $h = 1$.

Die Kettenbruchentwicklung der Reduzierten finden wir nach leichter Rechnung $(E(\sqrt{D}) = t + \frac{1}{2}a_1)$ zu:

$$\omega = c(2t + a_1) + c\left(-t - \frac{1}{2}a_1 + \sqrt{D}\right) = c(2t + a_1) + \cfrac{1}{t + \frac{1}{2}a_1 + \sqrt{D}}{c\left(a_2 - \frac{1}{4}a_1^2\right)},$$

$$\frac{t + \frac{1}{2}a_1 + \sqrt{D}}{c\left(a_2 - \frac{1}{4}a_1^2\right)} = \frac{2t + a_1}{c\left(a_2 - \frac{1}{4}a_1^2\right)} + \frac{1}{c\left(t + \frac{1}{2}a_1 + \sqrt{D}\right)} = \frac{2t + a_1}{c\left(a_2 - \frac{1}{4}a_1^2\right)} + \frac{1}{\omega}.$$

Also haben wir

$$+ \frac{1}{2}a_1 + \sqrt{D}\Big) = c(2t + a_1) + \cfrac{1}{\frac{2t + a_1}{c\left(a_2 - \frac{1}{4}a_1^2\right)} + \cfrac{1}{c(2t + a_1) + \cfrac{1}{\frac{2t + a_1}{c\left(a_2 - \frac{1}{4}a_1^2\right)} + \cdots}}}$$

Eine eingliedrige Periode gibt es unter den reduzierten Funktionen also nur, wenn $c = \frac{1}{c\left(a_2 - \frac{1}{4}a_1^2\right)}$ oder $a_2 - \frac{1}{4}a_1^2 = \frac{1}{c^2}$ ist. Wenn also $a_2 - \frac{1}{4}a_1^2$ quadratischer Rest ist.

Im Körper $K(\sqrt{D})$ ordnen wir nun wieder den reduzierten Funktionen $\omega = \frac{B + \sqrt{D}}{2C}$ das „reduzierte Ideal“

$$\mathfrak{a} = (2C, B + \sqrt{D})$$

zu. Dann gibt es in jeder Klasse reduzierte Ideale. Es gilt wieder $|N\mathfrak{a}| < |\sqrt{D}|$.

§ 14.

Die Einheiten des quadratischen Körpers.

Die ganze Funktion $\varepsilon = U + V\sqrt{D}$ ist dann und nur dann eine Einheit, wenn $N(\varepsilon) = c$ ist, wo c eine triviale Einheit ist.

Die Bestimmung aller Einheiten ist also äquivalent mit der Auflösung der „Pellschen Gleichung“

$$U^2 - V^2 D = c.$$

I. Der Körper $K(\sqrt{D})$ sei imaginär.

$$D = g, \qquad U^2 - V^2 g = c. \tag{1}$$

Da sich, wenn $|V| > 1$ ist, die höchsten Potenzen nicht wegheben können, muß v eine Zahl b und demnach auch U eine Zahl a sein.

Alle Einheiten haben also die Form

$$\varepsilon = a + b\sqrt{g},$$

wo a und b zwei nicht gleichzeitig verschwindende Zahlen sind.

Ihre Anzahl ist also $w = p^2 - 1$.

Ferner ist $N(\varepsilon) = a^2 - b^2 g$ und kann ersichtlich jede triviale Einheit sein. Die Anzahl der Einheiten gegebene Norm ist $p - 1$.

$$|D| \geqq p, \quad U^2 - V^2 D = c. \tag{2}$$

Wäre $V \neq 0$, so könnten sich wieder die höchsten Potenzen nicht heben. Aus $V = 0$ folgt aber, daß U eine triviale Einheit ist. Die trivialen Einheiten sind also hier die einzigen. Ihre Norm muß quadratischer Rest sein, und zu gegebener Norm gibt es zwei nur durch das Vorzeichen verschiedene Einheiten. Die Anzahl der Einheiten ist hier $w = p - 1$.

II. Der Körper $K(\sqrt{D})$ sei reell.

Sei ω eine zur Diskriminante D gehörige reduzierte Funktion. Wir entwickeln ω in einen Kettenbruch mit den Schlußfunktionen $\omega_1, \omega_2, \omega_3, \ldots$. Da er rein periodisch ist, muß unter ihnen schließlich einmal ω wieder auftreten. Sei etwa $\omega_n = \omega$. Dann ist

$$\omega = \frac{P_n \omega + P_{n-1}}{Q_n \omega + Q_{n-1}}$$

oder

$$Q_n \omega^2 - P_{n-1} = (P_n - Q_{n-1})\omega.$$

Vergleichen wir dies mit

$$C\omega^2 + A = B\omega,$$

so erhellt, da A, B, C ohne gemeinsamen Teiler sind, und ω irrational ist, daß die erste Gleichung aus der zweiten durch Multiplikation mit einer ganzen Funktion $2V$ hervorgeht. Da $n \geqq 1$, ist $Q_n \neq 0$, also auch $V \neq 0$. Wir haben also:

$$Q_n = 2VC, \qquad P_{n-1} = -2VA, \qquad P_n - Q_{n-1} = 2VB.$$

Setzen wir noch $P_n = VB + U$, so haben wir:

$$P_n = VB + U, \qquad Q_n = 2VC, \qquad P_{n-1} = -2VA, \qquad Q_{n-1} = -VB + U.$$

Der Identität

$$P_n Q_{n-1} - Q_n P_{n-1} = (-1)^n$$

entnehmen wir:

$$U^2 - V^2 B^2 + 4V^2 AC = (-1)^n, \text{ d. h. } U^2 - V^2 D = (-1)^n.$$

Es ist also

$$\varepsilon = U + V\sqrt{D}$$

eine Einheit, und zwar wegen $V \neq 0$ sicher keine triviale. Die Existenz nicht trivialer Einheiten im reellen Körper $K(\sqrt{D})$ ist also erwiesen.

Wir fragen nun nach Einheiten ε, deren Betrag $= 1$ ist. Aus $|\varepsilon| = 1$ und $|N(\varepsilon)| = |\varepsilon\varepsilon'| = 1$ folgt $|\varepsilon'| = 1$. Nun kann, wenn $V \neq 0$ ist, ersichtlich nicht gleichzeitig $|U + V\sqrt{D}| = 1$ und $|U - V\sqrt{D}| = 1$ sein. Denn sonst können sich die höchsten Potenzen nicht wegheben. Es ist also $V = 0$ und demnach ε eine triviale Einheit.

Die nicht trivialen Einheiten haben also stets einen Betrag $\neq 1$. Zwei Einheiten $\varepsilon_1, \varepsilon_2$ von gleichem Betrage $|\varepsilon_1| = |\varepsilon_2|$ sind durch eine Relation $\varepsilon_1 = a\varepsilon_2$ verbunden, wo a eine triviale Einheit ist. In der Tat ist $\frac{\varepsilon_1}{\varepsilon_2}$ auch eine Einheit und $\left|\frac{\varepsilon_1}{\varepsilon_2}\right| = 1$, so daß $\frac{\varepsilon_1}{\varepsilon_2} = a$ ist.

Da mit ε auch $\frac{1}{\varepsilon}$ eine Einheit ist, gibt es sicher Einheiten, deren Betrag > 1 ist. Von diesen seien die Einheiten $a\varepsilon_0$ jene mit dem kleinsten Betrag > 1. Die triviale Einheit a werde so gewählt, daß

$$N(a\varepsilon_0) = a^2 N(\varepsilon_0) = 1 \text{ oder } g$$

wird. Das Vorzeichen von a ist dabei noch beliebig und werde irgendwie fest gewählt. Die so normierte Einheit nennen wir die Grundeinheit des Körpers. Sie werde künftighin mit ε_0 bezeichnet. Es ist also $N(\varepsilon_0) = 1$ oder g.

Mit ε_0 sind auch alle Funktionen $\varepsilon = a \cdot \varepsilon_0^k$ (a eine Einheit, k irgendeine positive oder negative Zahl) Einheiten.

Satz. Jede Einheit von $K(\sqrt{D})$ hat die Form

$$\varepsilon = a \cdot \varepsilon_0^k.$$

Beweis. Wäre ε nicht in dieser Form enthalten, so müßte sich wegen $|\varepsilon_0| > 1$ eine Zahl ν so finden lassen, daß

$$|\varepsilon_0^\nu| < |\varepsilon| < |\varepsilon_0^{\nu+1}|.$$

Gleichheitszeichen könnten nicht stehen, da sich Einheiten gleichen Betrages nur um triviale Einheiten als Faktor unterscheiden, und somit ε doch in die Form $\varepsilon = a\varepsilon_0^k$ zu setzen wäre.

Aus unserer Ungleichung folgt

$$1 < |\varepsilon_0^{-\nu} \cdot \varepsilon| < |\varepsilon_0|.$$

Nun ist aber $\varepsilon_0^{-\nu}\varepsilon$ auch eine Einheit. Es gäbe also, entgegen der Definition der Grundeinheit, doch eine Einheit, deren Betrag zwischen 1 und $|\varepsilon_0|$ liegt. Widerspruch.

Für die Normen der Einheiten finden wir

$$N(\varepsilon) = a^2 (N(\varepsilon))^k = \begin{cases} a^2, & \text{wenn } N(\varepsilon_0) = 1, \\ a^2 g^k, & \text{wenn } N(\varepsilon_0) = g. \end{cases}$$

Wenn also $N(\varepsilon_0) = 1$ ist, sind die Normen quadratische Reste; für $N(\varepsilon_0) = g$ können sie jede rationale Einheiten sein.

Satz. Ist $K(\sqrt{D})$ ein reeller quadratischer Körper, wo D eine Primfunktion ist, und ist ε_0 seine Grundeinheit, so haben wir

$$N(\varepsilon_0) = g.$$

Beweis. Wäre $N(\varepsilon_0) = 1$, so könnten wir nach dem Hilfssatz des § 11 eine ganze Funktion β des Körpers finden, so daß $\varepsilon_0 = \frac{\beta'}{\beta}$ ist. Dann wäre $\beta' = \varepsilon_0 \beta$, also β und β' assoziiert. Es wäre also $(\beta) = (\beta')$, und somit (β) ein ambiges Hauptideal. Nach § 6 hat also (β) die Gestalt

$$\beta = (A)\, \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r,$$

wo die $\mathfrak{p}_\nu$ voneinander verschiedene Primideale sind, welche in der Diskriminante aufgehen. Da D Primfunktion ist, gibt es nur ein Primideal dieser Art:

$$\mathfrak{p} = (D, \sqrt{D}) = (\sqrt{D}).$$

A ist rational ganz. Also hat (β) eine der Formen

$$(\beta) = (A) \quad \text{oder} \quad \beta = A(\sqrt{D}).$$

Es ist also

$$\beta = A\varepsilon \quad \text{oder} \quad (\beta) = A\sqrt{D}\,\varepsilon,$$

wo ε eine Einheit ist, somit entweder

$$\varepsilon_0 = \frac{A\varepsilon'}{A\varepsilon} = \frac{\varepsilon'}{\varepsilon} = a \cdot \varepsilon'^2 \quad \text{oder} \quad \varepsilon_0 = \frac{-A\sqrt{D}\,\varepsilon'}{A\sqrt{D}\,\varepsilon} = -a\,\varepsilon'^2,$$

so daß ε_0 nicht die Grundeinheit wäre. Also ist $N(\varepsilon_0) = g$.

Nehmen wir ein Resultat des nächsten Paragraphen zu Hilfe, so gilt der

Satz. Wenn im reellen Körper $K(\sqrt{D})$ die Diskriminante D durch eine Primfunktion ungeraden Grades teilbar ist, gilt $N(\varepsilon_0) = 1$.

Beweis. Aus der Lösbarkeit der Pellschen Gleichung

$$U^2 - V^2 D = g$$

würde, wenn P unser Primteiler ungeraden Grades ist, die Lösbarkeit der Kongruenz

$$U^2 \equiv g \pmod{P}$$

folgen. Unabhängig von diesem Satz werden wir aber in § 15 zeigen, daß sie nicht lösbar ist. Also ist $N(\varepsilon_0) = 1$.

Nun beweisen wir (unabhängig von dem eben abgeleiteten Resultat) den

Satz. Die Klassenzahl des Körpers $K(\sqrt{D})$, wo D eine Primfunktion ist, ist ungerade, es sei denn, daß D einen geraden Grad hat, und der Körper imaginär ist (dann ist sie bekanntlich gerade).

Beweis. Wäre nämlich die Klassenzahl gerade, so müßte es mindestens eine von der Hauptklasse verschiedene ambige Klasse $\mathfrak{K}$ geben (deren Quadrat eben die Hauptklasse ist).

Dann gäbe es also ein Nichthauptideal $\mathfrak{a}$, für welches $\mathfrak{a} \sim \mathfrak{a}'$ ist, also $\frac{\mathfrak{a}'}{\mathfrak{a}} = \alpha$, wo α eine ganze oder gebrochene Funktion ist, deren Norm, wie man sich durch Normenbildung überzeugt, eine triviale Einheit a ist. Dabei ist α bis auf eine Körpereinheit festgelegt.

1. Grad von D ungerade. Wir setzen $\alpha = X + Y\sqrt{D}$. Dann soll $X^2 - Y^2 D = a$ sein, wo a eine triviale Einheit und X, Y rational ist. Da nun $Y^2 D$ auch ungeraden Grad hat, könnten sich, wenn $|Y^2 D| \geqq p$ wäre, die höchsten Potenzen von X^2 und $Y^2 D$ nicht heben. Es ist also $|Y^2 D| \leqq p^{-1}$, und somit $|X| = 1$. Daraus folgt

$$a = \operatorname{sgn}(X^2 - Y^2 D) = (\operatorname{sgn} X)^2 = b^2.$$

a ist also quadratischer Rest. Ersetzt man α durch das gleichwertige $\frac{\alpha}{b} = \alpha_1$, so hat man

$$\frac{\mathfrak{a}'}{\mathfrak{a}} = \alpha_1 \quad \text{mit} \quad N(\alpha_1) = 1.$$

2. Grad von D gerade, Körper reell, also $\operatorname{sgn} D = 1$. Sei ε_0 die Grundeinheit. Dann ist $N(\varepsilon_0) = g$. Wäre $N(\alpha)$ Nichtrest, so könnten wir α durch das gleichwertige $\varepsilon_0 \alpha$ ersetzen, dessen Norm dann ein Rest ist. Wir können also voraussetzen, es sei $N(\alpha) = b^2$. Ersetzen wir α durch das gleichwertige $\alpha_1 = \frac{\alpha}{b}$, so haben wir

$$\frac{\mathfrak{a}'}{\mathfrak{a}} = \alpha_1 \quad \text{mit} \quad N(\alpha_1) = 1.$$

Es gilt also in beiden Fällen

$$\frac{\mathfrak{a}'}{\mathfrak{a}} = \alpha_1 \quad \text{mit} \quad N(\alpha_1) = 1.$$

Dann gibt es ein ganzes β, so daß $\alpha_1 = \frac{\beta}{\beta'}$ ist, also

$$\mathfrak{a}\beta = (\mathfrak{a}\beta)'.$$

Das Ideal $\mathfrak{a}\beta$ wäre also ambig. Da D eine Primfunktion ist, hat also, wie schon einmal ausgeführt wurde, $\mathfrak{a}\beta$ entweder die Form (A) oder

$(A\sqrt{D})$. Es ist also auf jeden Fall $\mathfrak{a}\beta$ ein Hauptideal, also wegen $\mathfrak{a} \sim \mathfrak{a}\beta$ unsere Klasse $\mathfrak{K}$ die Hauptklasse, entgegen unserer Annahme.

Beispiel. Der reelle Körper $K(\sqrt{D})$ $(D = t^2 + a_1 t + a_2)$ hat die Grundeinheit

$$\varepsilon_0 = c\left(t + \frac{1}{2}a_1 + \sqrt{D}\right),$$

wo c passend gewählt ist. Seine Norm ist

$$N(\varepsilon_0) = c^2\left(\frac{1}{4}a_1^2 - a_2\right).$$

Da nun

$$D = \left(t + \frac{1}{2}a_1\right)^2 - \left(\frac{1}{4}a_1^2 - a_2\right)$$

ist, ist also $N(\varepsilon_0) = g$ oder 1, je nachdem ob D Primfunktion ist oder nicht. Wir bestätigen also unsere Sätze.

§ 15.

Das Reziprozitätsgesetz.

Wir wollen nun das von Dedekind ohne ausgeführten Beweis angegebene Reziprozitätsgesetz herleiten.

I. Der Ergänzungssatz.

Sei P eine primäre Primfunktion geraden Grades. Dann hat der reelle Körper $K(\sqrt{D})$ die Grundeinheit ε_0 mit der Norm $N(\varepsilon_0) = g$.

Die Pellsche Gleichung

$$X^2 - PY^2 = g$$

ist also lösbar und demnach erst recht die Kongruenz

$$X^2 \equiv g \pmod{P}.$$

Es ist also $\left[\frac{g}{P}\right] = +1$.

Im Körper $K(\sqrt{g})$ ist also die Primfunktion P zerlegbar in zwei (konjugierte) Primideale. Dieser Körper hat aber die Klassenzahl 1, so daß jedes Ideal ein Hauptideal ist. Demnach besteht eine Zerlegung der Form

$$P = (\alpha)\cdot(\alpha'),$$

wo $\alpha = X + Y\sqrt{g}$ eine ganze Funktion des Körpers $K(\sqrt{g})$ ist. Demnach ist

$$P = c(X^2 - gY^2),$$

wo X, Y ganz rational sind, und c eine triviale Einheit ist. P ist also darstellbar in dieser Form.

Sei nun P primär von ungeradem Grade. Wäre $\left[\frac{g}{P}\right] = -1$, so müßte sich P darstellen lassen in der Form

$$P = c(X^2 - gY^2).$$

Da sich die höchsten Potenzen der rechten Seite nicht heben können, ist der Grad der rechten Seite gerade. P kann sich also nicht durch diese Form darstellen lassen.

Es muß also, wenn P ungeraden Grad hat, $\left[\frac{g}{P}\right] = -1$ sein; die Kongruenz

$$X^2 \equiv g \pmod{P}$$

ist also unlösbar. Dies ist die im vorigen Paragraphen verwendete Behauptung.

Sei nun D_1 irgendeine ganze Funktion, Q einer ihrer Primteiler von ungeradem Grade. Sei D_1 darstellbar in der Form

$$D_1 = c(X^2 - gY^2).$$

Setzen wir $\alpha = X + Y\sqrt{g}$, so hat dies die Zerlegung

$$(D_1) = (\alpha)\cdot(\alpha')$$

zur Folge.

Im Körper $K(\sqrt{g})$ ist nun wegen $\left[\frac{g}{Q}\right] = -1$ der Primteiler Q selbst Primideal und geht demnach in einem der Faktoren rechter Hand auf. Da er ein ambiges Primideal ist, geht er in jedem der konjugierten Ideale (α) und (α') gleich oft auf. In D_1 muß er demnach in gerader Potenz aufgehen. Soll sich also D_1 durch unsere Form darstellen lassen, so darf D_1 Primfunktionen ungeraden Grades nur in gerader Potenz enthalten. Ist dies aber der Fall, so können wir D_1 in die Form setzen

$$D_1 = a P_1 P_2 \dots P_n \cdot A^2,$$

wo a eine Einheit, P_ν Primfunktionen geraden Gerades und A eine ganze rationale Funktion sind.

Sei nun

$$P_\nu = c_\nu (X_\nu + Y_\nu\sqrt{g})(X_\nu - Y_\nu\sqrt{g}).$$

Setzen wir

$$A(X_1 + Y_1\sqrt{g})(X_2 + Y_2\sqrt{g}) \dots (X_n + Y_n\sqrt{g}) = X + Y\sqrt{g}$$

und $c = a c_1 c_2 \dots c_n$, so ist

$$D_1 = c(X^2 - Y^2 g).$$

Eine Funktion D_1 ist also dann und nur dann in unserer Form darstellbar, wenn D_1 Primfaktoren ungeraden Grades nur in gerader Potenz enthält.

Ist D_1 speziell quadratfrei, so haben wir den in § 11 verwendeten Satz über die Darstellbarkeit quadratfreier Funktionen durch unsere Form bewiesen.

Sei P eine beliebige primäre Primfunktion. Da stets $\left[\frac{b^2}{P}\right] = +1$ ist, erhält man den Ergänzungssatz:

$$\left[\frac{a}{P}\right] = \left(\frac{a}{p}\right)^r$$

wo $\left(\frac{a}{p}\right)$ das Legendresche Symbol ist.

II. Das Reziprozitätsgesetz für primäre Primfunktionen P und Q.

1. Wenigstens eine der beiden Primfunktionen hat geraden Grad.

Sei $\left[\frac{P}{Q}\right] = +1$. Wir betrachten den Körper $K(\sqrt{P})$. Da $\operatorname{sgn} P = 1$ ist, ist seine Klassenzahl sicher ungerade: $h = 2k+1$. Q ist wegen $\left[\frac{P}{Q}\right] = +1$ im Körper zerlegbar in zwei konjugierte Primideale: $Q = \mathfrak{q}\,\mathfrak{q}'$. Sei $\mathfrak{K}$ die Klasse, der $\mathfrak{q}$ angehört. Nach dem Fermatschen Satze der Gruppentheorie ist $\mathfrak{K}^h$ die Hauptklasse, also $\mathfrak{q}^{2k+1}$ ein Hauptideal (α), wo $\alpha = X + Y\sqrt{P}$ ganz ist. Somit $\mathfrak{q}'^{2k+1} = (\alpha')$. Dies liefert

$$Q^{2k+1} = (\alpha\cdot\alpha') = (X^2 - Y^2 P),$$

also

$$Q^{2k+1} = c\cdot(X^2 - Y^2\cdot P),$$

wo c eine triviale Einheit.

a) Grad von P ungerade. Dann ist Q von geradem Grade, also auch Q^{2k+1}. Da nun rechter Hand $Y^2 P$ ungeraden, X^2 aber geraden Grad hat, ist $|X^2| > |Y^2 P|$, und wegen

$$\operatorname{sgn} Q = 1 \quad \text{muß sein} \quad 1 = c\,(\operatorname{sgn} X)^2,$$

also c quadratischer Rest: $c = a^2$. Schreiben wir $\frac{X}{a}$, $\frac{Y}{a}$ an Stelle von X und Y, so wird also

$$Q^{2k+1} = X^2 - Y^2\cdot P.$$

b) Grad von P gerade. Sei $\varepsilon_0 = U + V\sqrt{P}$ die Grundeinheit von $K(\sqrt{P})$. Dann ist $N(\varepsilon_0) = g$. Setzen wir

$$\varepsilon_0\,(X + Y\sqrt{P}) = X_1 + Y_1\sqrt{P},$$

so haben wir

$$Q^{2k+1} - c\,(X^2 - Y^2 P) = \frac{c}{N(\varepsilon_0)}\,(X_1^2 - Y_1^2 P) = \frac{c}{g}\cdot(X_1^2 - Y_1^2 P).$$

Nun ist eine der beiden Zahlen c und $\frac{c}{g}$ sicher Rest. Wir können also annehmen, c sei quadratischer Rest: $c = a^2$. Ersetzen wir wieder X und Y durch $\frac{X}{a}$, $\frac{Y}{a}$, so wird

$$Q^{2k+1} = X^2 - Y^2 P.$$

In beiden Fällen erkennen wir, wenn wir die Gleichungen als Kongruenzen schreiben, daß die Kongruenz

$$X^2 \equiv Q^{2k+1} \pmod{P}$$

lösbar ist. Es ist also $\left[\frac{Q^{2k+1}}{P}\right] = +1$ und nach den Multiplikationsregeln, die bei Dedekind angegeben sind,

$$\left[\frac{Q}{P}\right]^{2k+1} = \left[\frac{Q}{P}\right] = +1.$$

Daraus folgt, daß mit $\left[\frac{P}{Q}\right] = -1$ auch $\left[\frac{Q}{P}\right] = -1$ sein muß, da sonst rückschließend ein Widerspruch entstünde. Es ist also $\left[\frac{P}{Q}\right] = \left[\frac{Q}{P}\right]$, wenn wenigstens eine der Primfunktionen geraden Grad hat.

2. P und Q haben ungeraden Grad.

Wenn hier $\left[\frac{P}{Q}\right] = (-1)^n$ ist ($n = 0$ oder 1), so ist nach dem Ergänzungssatz und den Multiplikationsregeln

$$\left[\frac{g^n P}{Q}\right] = \left[\frac{g}{Q}\right]^n \cdot \left[\frac{P}{Q}\right] = (-1)^n \cdot (-1)^n = +1.$$

Es ist also Q im Körper $K(\sqrt{g^n P})$, dessen Klassenzahl des ungeraden Grades von P wegen sicher ungerade $= 2k+1$ ist, zerlegbar: $Q = \mathfrak{q}\,\mathfrak{q}'$. Wieder ist $\mathfrak{q}^{2k+1}$ ein Hauptideal (α), wo $\alpha = X + Y\sqrt{g^n P}$ eine ganze Funktion von $K(\sqrt{g^n P})$ ist. Man erhält wieder

$$Q^{2k+1} = c\,(X^2 - Y^2 g^n P).$$

Q^{2k+1} hat ungeraden, X^2 geraden Grad. Diesmal rührt also der höchste Koeffizient rechter Hand von $Y^2 g^n P$ her. Wegen

$$\operatorname{sgn} P = \operatorname{sgn} Q = 1 \quad \text{ist also} \quad 1 = -c\,g^n (\operatorname{sgn} Y)^2.$$

c hat also die Form $c = -g^{-n} a^2$.

Ersetzt man wieder X und Y durch $\frac{X}{a}$ und $\frac{Y}{a}$, so wird

$$Q^{2k+1} = -g^{-n}(X^2 - Y^2 g^n P).$$

Dies zeigt also die Lösbarkeit der Kongruenz

$$X^2 \equiv -g^n Q^{2k+1} \pmod{P},$$

so daß

$$\left[\frac{-g^n Q^{2k+1}}{P}\right] = +1, \quad \text{also} \quad \left[\frac{Q}{P}\right]^{2k+1} = \left[\frac{-1}{P}\right] \cdot \left[\frac{g^n}{P}\right].$$

Wir haben also

$$\left[\frac{Q}{P}\right] = \left[\frac{Q}{P}\right]^{2k+1} = \left(\frac{-1}{p}\right) \cdot (-1)^n = \left(\frac{-1}{p}\right) \cdot \left[\frac{P}{Q}\right].$$

Im ganzen ist also

$$\left[\frac{P}{Q}\right]\cdot\left[\frac{Q}{P}\right]=1 \quad \text{oder} \quad \left(\frac{-1}{p}\right),$$

je nachdem wenigstens eine der Primfunktionen geraden Grad hat oder beide ungeraden Grades sind.

Nennen wir also die Grade μ und ν, so ist damit das Reziprozitätsgesetz bewiesen:

$$\left[\frac{P}{Q}\right]\cdot\left[\frac{Q}{P}\right]=\left(\frac{-1}{p}\right)^{\mu\nu}.$$

§ 16.

Verallgemeinerung.

Seien nun M und N zwei beliebige teilerfremde Funktionen, davon N primär. $N=Q_1Q_2\ldots$ sei die Zerlegung von N in Primfunktionen.

Wir führen nun das dem Jacobischen entsprechende Symbol ein:

$$\left[\frac{M}{N}\right]=\prod_i\left[\frac{M}{Q_i}\right].$$

Das Symbol hat folgende Eigenschaften, die unmittelbar aus denen von $\left[\frac{M}{Q}\right]$ folgen:

1. $\left[\frac{M_1}{N}\right]\cdot\left[\frac{M_2}{N}\right]=\left[\frac{M_1M_2}{N}\right]$, weil $\left[\frac{M_1}{Q_i}\right]\cdot\left[\frac{M_2}{Q_i}\right]=\left[\frac{M_1M_2}{Q_i}\right]$.

2. Sei

$$M_1\equiv M_2 \pmod N.$$

Dann ist erst recht

$$M_1\equiv M_2 \pmod{Q_i}, \quad \text{also} \quad \left[\frac{M_1}{Q_i}\right]=\left[\frac{M_2}{Q_i}\right].$$

Es ist also

$$\left[\frac{M_1}{N}\right]=\left[\frac{M_2}{N}\right].$$

3. Es sei auch $M=P_1P_2\ldots$ primär. $\mu_1,\mu_2,\ldots$ seien die Grade von $P_1,P_2,\ldots$, $\nu_1,\nu_2,\ldots$ die von $Q_1,Q_2,\ldots$, μ sei der von M und ν der von N. Dann ist:

$$\mu=\sum_i\mu_i, \quad \nu=\sum_k\nu_k, \quad \text{also} \quad \mu\nu=\sum_{i,k}\mu_i\nu_k.$$

Wegen

$$\left[\frac{N}{M}\right]=\prod_{i,k}\left[\frac{Q_k}{P_i}\right], \quad \left[\frac{M}{N}\right]=\prod_{i,k}\left[\frac{P_i}{Q_k}\right]$$

gilt

$$\left[\frac{N}{M}\right]\left[\frac{M}{N}\right]=\prod_{i,k}\left(\frac{-1}{p}\right)^{\mu_i\nu_k}=\left(\frac{-1}{p}\right)^{\sum_{i,k}\mu_i\nu_k}=\left(\frac{-1}{p}\right)^{\mu\nu}.$$

Ferner ist

$$\left[\frac{a}{M}\right] = \Pi\left[\frac{a}{P_i}\right] = \prod_i \left(\frac{a}{p}\right)^{\mu_i} = \left(\frac{a}{p}\right)^{\mu}.$$

Ist also M und N primär und teilerfremd, so gilt das Reziprozitätsgesetz (wenn μ und ν die Grade sind)

$$\left[\frac{M}{N}\right]\left[\frac{N}{M}\right] = \left(\frac{-1}{p}\right)^{\mu\nu}$$

und der Ergänzungssatz

$$\left[\frac{a}{M}\right] = \left(\frac{a}{p}\right)^{\mu}.$$

Die Symbole $\left[\frac{M}{N}\right]$ und $\left[\frac{N}{M}\right]$ sind also dann und nur dann verschieden, wenn gleichzeitig M und N ungeraden Grad haben und $p \equiv 3 \pmod 4$ ist.

Beachten wir

$$\frac{|M|-1}{p-1} = \frac{p^{\mu}-1}{p-1} = 1 + p + p^2 + \ldots + p^{\mu-1} \equiv \mu \pmod 2$$

und analog

$$\frac{|N|-1}{p-1} \equiv \nu \pmod 2,$$

sowie

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\left(\frac{p-1}{2}\right)^2} \quad \text{und} \quad \left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$$

(Eulersches Kriterium), so können wir dem Gesetz die Form geben:

$$\left[\frac{M}{N}\right]\left[\frac{N}{M}\right] = (-1)^{\frac{|M|-1}{2}\cdot\frac{|N|-1}{2}}, \qquad \left[\frac{a}{M}\right] = a^{\frac{|M|-1}{2}},$$

in der die Analogie mit dem gewöhnlichen Reziprozitätsgesetze am deutlichsten ist.

Sei nun Δ eine primäre Funktion, die nicht gerade ein volles Quadrat ist. Dann enthält Δ mindestens eine Primfunktion P in ungerader Potenz. Wir setzen $\Delta = P^{2k+1}\Delta_1$, wo Δ_1 prim zu P ist. Nach Dedekind besitzt P mindestens einen Nichtrest B. Wir bestimmen nun die zu Δ prime Funktion F durch die Kongruenzen

$$F \equiv B \pmod P, \qquad F \equiv 1 \pmod{\Delta_1},$$

was immer geht. Dann ist

$$\left[\frac{F}{\Delta}\right] = \left[\frac{F}{P}\right]^{2k+1} \cdot \left[\frac{F}{\Delta_1}\right] = \left[\frac{B}{P}\right]^{2k+1} = -1.$$

Nun betrachten wir die Summe

$$S = \sum_{(G,\Delta)=1} \left[\frac{G}{\Delta}\right],$$

erstreckt über ein Repräsentantensystem der primen Restklassen modulo Δ.

Mit G durchläuft dann auch FG ein solches Repräsentantensystem. Es ist also

$$S = \sum_{(G,\,\Delta)=1} \left[\frac{FG}{\Delta}\right] = \left[\frac{F}{\Delta}\right] \cdot \sum_{(G,\,\Delta)=1} \left[\frac{G}{\Delta}\right] = -S.$$

Daraus folgt

$$S = 0.$$

Wenn also Δ kein volles Quadrat ist, verschwindet $\sum \left[\frac{G}{\Delta}\right]$ erstreckt über ein Repräsentantensystem primer Restklassen.

Es sei nun $K(\sqrt{D})$ irgendein Körper. Dann führen wir die Größen ein:

$$\sigma_\nu = \sum_{|F|=p^\nu} \left[\frac{D}{F}\right],$$

wo die Summe über alle primären, zu D primen Funktionen F vom ν-ten Grad zu erstrecken ist.

Satz. Ist $D \neq g$ und D vom n-ten Grade, so gilt

$$\sigma_\nu = 0 \quad \text{für} \quad \nu \geqq n.$$

Beweis. Wir setzen $D = a\Delta$, wo $a = \operatorname{sgn} D$ ist. Dann ist Δ wegen $D \neq g$ quadratfrei und primär, also sicher kein volles Quadrat.

Nach dem Reziprozitätsgesetze ist nun (ν Grad von F)

$$\left[\frac{D}{F}\right] = \left[\frac{a}{F}\right]\left[\frac{\Delta}{F}\right] = \left(\frac{a}{p}\right)^\nu \cdot \left(\frac{-1}{p}\right)^{\nu n} \cdot \left[\frac{F}{\Delta}\right].$$

Setzen wir also $b = a \cdot (-1)^n$, so wird

$$\left[\frac{D}{F}\right] = \left(\frac{b}{p}\right)^\nu \cdot \left[\frac{F}{\Delta}\right].$$

Sei nun $\nu \geqq n$. Dann hat F die Form $F = K \cdot \Delta + A$, wo $|A| < \Delta$ und K ganz, primär und von Null verschieden ist. F durchläuft nun alle primären zu Δ primen Funktionen des Grades ν, wenn A alle zu Δ primen (nicht nur primären) Funktionen niedrigeren Grades als Δ (also ein Repräsentantensystem primer Restklassen) durchläuft, und gleichzeitig unabhängig K alle ganzen primären Funktionen $(\nu - n)$-ten Grades. Für $\nu \geqq n$ ist also

$$\sigma_\nu = \sum_{|F|=p^\nu} \left[\frac{D}{F}\right] = \left(\frac{b}{p}\right)^\nu \cdot \sum_{|K|=p^{\nu-n}} \sum_{\substack{(A,\,\Delta)=1 \\ |A|<\Delta}} \left[\frac{K\Delta + A}{\Delta}\right] = \left(\frac{b}{p}\right)^\nu \cdot \sum_A \left[\frac{A}{\Delta}\right] \cdot \sum_K 1.$$

Nach dem vorhin Gezeigten gilt also die Behauptung.

(Eingegangen am 14. Oktober 1921.)

Quadratische Körper im Gebiete der höheren Kongruenzen. II.

(Analytischer Teil.)*)

Von

E. Artin in Hamburg.

§ 17.

Die Zetafunktionen.

Analog zur Funktion $\zeta(s)$ in Zahlkörpern führen wir ein

$$Z(s) = \sum_{\mathfrak{a}} \frac{1}{|N\mathfrak{a}|^s},$$

die Summe erstreckt über alle Ideale von $K(\sqrt{D})$. Wollen wir dabei die Abhängigkeit vom Körper zum Ausdruck bringen, so schreiben wir $Z_D(s)$.

Um die Konvergenz dieser Reihe zu untersuchen, betrachten wir das Produkt

$$\prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{|N\mathfrak{p}|^s}},$$

erstreckt über alle Primideale von $K(\sqrt{D})$.

Dieses Produkt ist für $\Re(s) \geqq 1 + \delta$ absolut und gleichmäßig konvergent. Denn wenn $\mathfrak{p}$ ein Teiler der primären Primfunktion P ist, ist $|N\mathfrak{p}| \geqq |P|$, und zu jedem P gehören höchstens zwei Primideale. Also ist für $\Re(s) \geqq 1 + \delta$

$$\sum_{\mathfrak{p}} \left| \frac{1}{|N\mathfrak{p}|^s} \right| \leqq \sum_{P} \frac{2}{|P|^{\Re(s)}} < 2 \sum_{F} \frac{1}{|F|^{1+\delta}} \qquad (\operatorname{sgn} F = 1),$$

*) Vgl. E. Artin, Quadratische Körper im Gebiete der höheren Kongruenzen. I. (Arithmetischer Teil.) Math. Zeitschr. **19** (1924), S. 153–206.

wo die letzte Summe über alle Funktionen erstreckt ist. Also

$$\sum_{\mathfrak{p}} \left| \frac{1}{|N\mathfrak{p}|^s} \right| < 2 \sum_{\nu} \frac{p^\nu}{p^{\nu(1+\delta)}} = 2 \sum_{\nu} p^{-\nu\delta}.$$

Die letzte Summe ist aber eine konvergente geometrische Reihe.

Wie in Zahlkörpern weist man nun die Identität

$$\prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{|N\mathfrak{p}|^s}} = \sum_{\mathfrak{a}} \frac{1}{|N\mathfrak{a}|^s}$$

nach, und daß auch die Reihe für $\Re(s) \geqq 1 + \delta$ absolut und gleichmäßig konvergiert.

Für $\Re(s) > 1$ ist also $Z(s)$ regulär, und es gilt

$$(1) \qquad Z(s) = \sum_{\mathfrak{a}} \frac{1}{|N\mathfrak{a}|^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{|N\mathfrak{p}|^s}}.$$

Nunmehr unterscheiden wir unsere drei Arten von Primidealen:

1. $\mathfrak{p}\mathfrak{p}' = P$, $\mathfrak{p} \neq \mathfrak{p}'$. Dann ist P prim zu D und $\left[\frac{D}{P}\right] = +1$ (P primär). Die zu P gehörigen Primideale liefern im Produkt den Beitrag

$$\frac{1}{1 - \frac{1}{|N\mathfrak{p}|^s}} \cdot \frac{1}{1 - \frac{1}{|N\mathfrak{p}'|^s}} = \frac{1}{1 - \frac{1}{|P|^s}} \cdot \frac{1}{1 - \frac{1}{|P|^s}} = \frac{1}{1 - \frac{1}{|P|^s}} \cdot \frac{1}{1 - \frac{\left[\frac{D}{P}\right]}{|P|^s}}.$$

2. $\mathfrak{p} = \mathfrak{p}' = P$, also die primäre Primfunktion P selbst Primideal. Dann ist $\left[\frac{D}{P}\right] = -1$ und $N\mathfrak{p} = P^2$. Als Beitrag kommt

$$\frac{1}{1 - \frac{1}{|N\mathfrak{p}|^s}} = \frac{1}{1 - \frac{1}{|P|^{2s}}} = \frac{1}{1 - \frac{1}{|P|^s}} \cdot \frac{1}{1 + \frac{1}{|P|^s}} = \frac{1}{1 - \frac{1}{|P|^s}} \cdot \frac{1}{1 - \frac{\left[\frac{D}{P}\right]}{|P|^s}}.$$

3. P ein Teiler von D. Dann ist $P = \mathfrak{p}^2$ und $N\mathfrak{p} = P$. Also erhalten wir als Beitrag

$$\frac{1}{1 - \frac{1}{|N\mathfrak{p}|^s}} = \frac{1}{1 - \frac{1}{|P|^s}}.$$

Bilden wir das Produkt über alle primären Primfunktionen, so können wir das erste Glied der Beiträge 1 und 2 mit dem dritten Beitrag zu $\prod_P \frac{1}{1 - \frac{1}{|P|^s}}$ vereinigen, wo das Produkt über alle primären Primfunktionen zu erstrecken ist. Es erhält aber nun nach einfacher Umformung den

Wert $\sum_F \frac{1}{|F|^s}$, erstreckt über alle primären ganzen Funktionen. Vereinigen wir die Glieder gleichen Grades, so erhalten wir

$$\sum \frac{1}{|F|^s} = \sum_{\nu=0}^{\infty} p^{\nu} \cdot p^{-\nu s} = \frac{1}{1-p^{-(s-1)}}.$$

Demnach ergibt sich

$$(2) \qquad Z(s) = \frac{1}{1-p^{-(s-1)}} \cdot \prod_{(P,D)=1} \frac{1}{1-\left[\frac{D}{P}\right]\frac{1}{|P|^s}},$$

wo das letzte Produkt über alle zu D primen primären Primfunktionen zu erstrecken ist.

Die Eulersche Umformung des Produktes ergibt

$$(3) \qquad Z(s) = \frac{1}{1-p^{-(s-1)}} \cdot \sum_F \left[\frac{D}{F}\right] \frac{1}{|F|^s} \quad \text{für} \quad \Re(s) > 1,$$

wo die letzte Summe über alle zu D primen primären Funktionen zu erstrecken ist.

Vereinigen wir alle Funktionen gleichen Grades, so wird

$$Z(s) = \frac{1}{1-p^{-(s-1)}} \cdot \sum_{\nu=0}^{\infty} \frac{\sigma_\nu}{p^{\nu s}},$$

wo σ_ν die im vorigen Paragraphen eingeführten Größen sind:

$$(4) \qquad \sigma_\nu = \sum_{|F|=p^\nu} \left[\frac{D}{F}\right] \quad \text{mit } \operatorname{sgn} F = 1,\ D, F \text{ relativ prim.}$$

1. $D \neq g$. Dann hätten wir $\sigma_\nu = 0$ für $\nu \geqq n$ gezeigt. Es kommen also nur die Größen $\sigma_0, \sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ in Betracht. Dabei ist n der Grad von D, der nun immer so bezeichnet werde. Unter σ_ν wollen wir weiterhin nur diese Zahlen verstehen. Dabei ist $\sigma_0 = 1$. Es wird also

$$(5) \qquad Z(s) = \frac{1}{1-p^{-(s-1)}} \cdot \sum_{\nu=0}^{n-1} \frac{\sigma_\nu}{p^{\nu s}}.$$

Die Zetafunktion ist also in der ganzen Ebene mit eventueller Ausnahme der Stellen $s = 1 + \frac{2k\pi i}{\log p}$ (k ganz), welche Pole sein können, regulär.

Ferner ist ersichtlich $Z(s)$ periodisch mit der Periode $\frac{2\pi i}{\log p}$, eine Eigenschaft, die später sehr nützlich sein wird.

Die Zahlen σ_ν zeichnen sich, wie bald gezeigt werden soll, durch höchst merkwürdige Reziprozitätsbeziehungen aus. Wir werden überhaupt sehen, daß sie eine wichtige Stellung in der Theorie einnehmen.

Für jetzt seien noch einige elementare Eigenschaften der Zahlen σ_r hergeleitet. Wollen wir ihre Abhängigkeit vom Körper kennzeichnen, so schreiben wir $\sigma_r(D)$.

Aus dem Ergänzungssatz des Reziprozitätsgesetzes folgt leicht

$$\sigma_r(gD) = (-1)^r \sigma_r(D). \tag{6}$$

Ist ferner $K(\sqrt{D})$ reell, so ist $\operatorname{sgn} D = 1$, also

$$\sum_{(A,D)=1} \left[\frac{A}{D}\right] = 0.$$

wenn A ein Repräsentantensystem der primen Restklassen, etwa alle Funktionen niedrigeren Grades als D, welche zu D relativ prim sind, durchläuft. Dies ist der Fall, wenn in $A = aF$, F alle zu D primen Funktionen mit $|F| < |D|$ und a alle trivialen Einheiten durchläuft.

Dann ist aber, weil D geraden Grad hat,

$$\left[\frac{A}{D}\right] = \left[\frac{a}{D}\right]\left[\frac{F}{D}\right] = \left[\frac{D}{F}\right].$$

Also

$$\sum \left[\frac{A}{D}\right] = \sum_{a=1}^{p-1} \sum_{F} \left[\frac{D}{F}\right] = (p-1) \sum_{F} \left[\frac{D}{F}\right].$$

Somit ist

$$\sum_{\substack{|F|<|D| \\ \operatorname{sgn} F = 1}} \left[\frac{D}{F}\right] = 0.$$

Ordnen wir nach Graden, so erhalten wir den

Satz. Wenn $K(\sqrt{D})$ reell ist, gilt:

$$\sigma_0 + \sigma_1 + \sigma_2 + \ldots + \sigma_{n-1} = 0. \tag{7}$$

Wir werden bald sehen, daß dies auch nur in diesem Falle gilt, denn in jedem anderen wird sich die Summe als die Klassenzahl herausstellen und ist also wesentlich positiv.

Für $Z(s)$ ergeben sich daraus zwei elementare Eigenschaften. Zunächst ist nämlich

$$Z_D\left(s + \frac{\pi i}{\log p}\right) = \frac{1}{1 + p^{-(s-1)}} \left(1 - \frac{\sigma_1(D)}{p^s} + \frac{\sigma_2(D)}{p^{2s}} - + \ldots + (-1)^{n-1} \frac{\sigma_{n-1}(D)}{p^{(n-1)s}}\right).$$

Aus (6) aber folgt

$$Z_D(s) = \frac{1}{1 - p^{-(s-1)}} \left(1 - \frac{\sigma_1(D)}{p^s} + \frac{\sigma_2(D)}{p^{2s}} - + \ldots + (-1)^{n-1} \frac{\sigma_{n-1}(D)}{p^{(n-1)s}}\right).$$

Wir erhalten also durch Division die Funktionalgleichung

$$Z_D\left(s + \frac{\pi i}{\log p}\right) = \frac{1 - p^{-(s-1)}}{1 + p^{-(s-1)}} \cdot Z_{gD}(s). \tag{8}$$

Aus (7) folgt ferner, daß $Z_D(s)$ für reelle Körper $K(\sqrt{D})$ in $s=0$ eine Nullstelle besitzt. Aus (8) folgt dann weiter, daß $Z_D(s)$ für imaginäre Körper, deren Diskriminante geraden Grad hat, in $s=\frac{\pi i}{\log p}$ eine Nullstelle hat.

Der Periodizität wegen sind natürlich auch die um $\frac{2k\pi i}{\log p}$ vermehrten Stellen Nullstellen.

Endlich finden wir allgemein

$$Z(0) = -\frac{1}{p-1}\cdot\sum_{\nu=0}^{n-1}{}'\sigma_\nu, \tag{9}$$

$$\lim_{s=1}(s-1)Z(s) = \frac{1}{\log p}\cdot\sum_{\nu=0}^{n-1}{}'\frac{\sigma_\nu}{p^\nu}. \tag{10}$$

2. Für $D=g$ ist $\sigma_\nu = p^\nu\cdot(-1)^\nu$, also finden wir

$$Z_g(s) = \frac{1}{1-p^{-(s-1)}}\cdot\frac{1}{1+p^{-(s-1)}}, \tag{11}$$

sowie

$$Z(0) = -\frac{1}{p^2-1}, \qquad \lim_{s=1}(s-1)Z(s) = \frac{1}{2\log p}.$$

Außer der Funktion $Z(s)$ führen wir noch ein die „Zetafunktion der Klasse $\mathfrak{K}$“: $Z(s,\mathfrak{K})$.

Sei nämlich $\mathfrak{K}$ eine Idealklasse von $K(\sqrt{D})$, dann setzen wir ($\mathfrak{a}$ durchlaufe alle Ideale aus $\mathfrak{K}$):

$$Z(s,\mathfrak{K}) = \sum_{\mathfrak{a}\text{ aus }\mathfrak{K}}{}'\frac{1}{|N\mathfrak{a}|^s}. \tag{12}$$

Die Reihe konvergiert, da sie einen Teil der Reihe von $Z(s)$ darstellt, absolut und gleichmäßig für $\Re(s)\geqq 1+\delta$.

Ferner ist klar, daß

$$Z(s) = \sum_{\mathfrak{K}}{}'Z(s,\mathfrak{K}), \tag{13}$$

erstreckt über alle Idealklassen.

Nun sei $\mathfrak{a}$ ein Ideal der Klasse $\mathfrak{K}^{-1}=\mathfrak{K}'$. Wenn dann $\mathfrak{b}$ ein Ideal aus $\mathfrak{K}$ ist, ist $\mathfrak{a}\mathfrak{b}$ ein Hauptideal (α). Und umgekehrt, wenn das Hauptideal (α) durch $\mathfrak{a}$ teilbar ist, ist $(\alpha)=\mathfrak{a}\mathfrak{b}$ und $\mathfrak{b}$ ein Ideal aus $\mathfrak{K}$. $\mathfrak{a}\mathfrak{b}$ durchläuft also alle durch $\mathfrak{a}$ teilbaren Hauptideale, wenn $\mathfrak{b}$ die Ideale aus $\mathfrak{K}$ durchläuft. Es ist daher

$$Z(s,\mathfrak{K}) = |N\mathfrak{a}|^s\cdot\sum_{\mathfrak{b}\text{ aus }\mathfrak{K}}{}'\frac{1}{|N\mathfrak{a}\mathfrak{b}|^s} = |N\mathfrak{a}|^s\sum_{\alpha\equiv 0\,(\mathrm{mod}\,\mathfrak{a})}{}'\frac{1}{|N\alpha|^s},$$

wo der Akzent anzeigt, daß über alle nicht assoziierten Funktionen des Ideals $\mathfrak{a}$ summiert wird. Da nun aber ersichtlich $Z(s,\mathfrak{K})=Z(s,\mathfrak{K}')$ ist, kann $\mathfrak{a}$ auch als in $\mathfrak{K}$ gelegen angenommen werden.

Satz. Ist $\mathfrak{a}$ ein beliebiges Ideal aus $\mathfrak{K}$, so gilt

$$Z(s,\mathfrak{K}) = |N\mathfrak{a}|^s \sum_{\alpha \equiv 0 \,(\mathrm{mod}\,\mathfrak{a})}{}' \frac{1}{|N\alpha|^s}, \tag{14}$$

die Summe erstreckt über alle nicht assoziierten Funktionen des Ideals $\mathfrak{a}$ ($\alpha \neq 0$).

§ 18.

Die Anzahl der Idealklassen im imaginären Körper.

Im imaginären Körper $K(\sqrt{D})$ gibt es nur endlich viele Einheiten. Nennen wir ihre Anzahl w (es ist $w = p^2 - 1$ für $D = g$, sonst $w = p - 1$), so finden wir aus (14), da assoziierte Funktionen die gleiche absolute Norm besitzen,

$$Z(s,\mathfrak{K}) = \frac{|N\mathfrak{a}|^s}{w} \cdot \sum_{\alpha \equiv 0 \,(\mathrm{mod}\,\mathfrak{a})} \frac{1}{|N\alpha|^s}, \tag{1}$$

wo jetzt die Summationsbeschränkung bis auf $\alpha \neq 0$ aufgehoben ist.

Es werde nun $\mathfrak{a}$ als reduziertes Ideal der Klasse $\mathfrak{K}$ gewählt. Dies geht; denn in jeder Klasse gibt es reduzierte Ideale.
Dann hat $\mathfrak{a}$ eine Basisdarstellung

$$\mathfrak{a} = (2C, B + \sqrt{D}), \qquad D = B^2 - 4AC,$$

wo

$$|B| < |C| \leqq \sqrt{|D|}. \tag{2}$$

Ferner folgt aus (2)

$$|D| = |AC| \quad \text{und} \quad |N\mathfrak{a}| = |C|. \tag{3}$$

Es ist nun

$$\alpha = 2CX + (B + \sqrt{D})Y,$$
$$\alpha' = 2CX + (B - \sqrt{D})Y,$$

also

$$N\alpha = (2CX + BY)^2 - DY^2,$$

wo X, Y ganze, nicht gleichzeitig verschwindende Funktionen sind.

Dann ist

$$Z(s,\mathfrak{K}) = \frac{|C|^s}{w} \cdot \sum_{X,Y}{}' \frac{1}{|(2CX + BY)^2 - DY^2|^s}. \tag{4}$$

Es bestehen nun zwei Möglichkeiten:

1. $$|2BX + BY|^2 > |DY^2|,$$

so daß

$$|(2CX + BY)^2 - DY^2| = |2CX + BY|^2.$$

Dann ist für $Y \neq 0$

$$\left|2C\frac{X}{Y}+B\right| > \sqrt{|D|};$$

wegen $|B| < \sqrt{|D|}$ muß also

$$\left|2C\frac{X}{Y}\right| > \sqrt{|D|}$$

sein. Ist umgekehrt dies der Fall, so gelangen wir zur Ausgangsrelation. Wegen $|B| < \sqrt{|D|}$ ist dann

$$|CX| > |BY|,$$

so daß

$$|2CX+BY|^2 = |CX|^2, \quad \text{also} \quad |N\alpha| = |CX|^2$$

ist. Im Falle $Y = 0$ ist dies ohne weiteres klar. Wir haben also: Für

(5) $$|CX^2| > |AY^2| \quad \text{gilt} \quad |N\alpha| = |CX|^2$$

und nur dann. Es folgt dies nämlich leicht aus $|D| = |AC|$.

2. $$|2CX^2+BY|^2 \leqq |DY^2| = |ACY^2|,$$

so daß

$$|(2CX+BY)^2 - DY^2| = |ACY^2|.$$

Dies ist, da $\sqrt{|D|}$ imaginär ist, auch im Falle des Gleichheitszeichens richtig. Hier kann Y nur mit X verschwinden, was nicht geht. Es ist also $Y \neq 0$, also

$$\left|2C\frac{X}{Y}+B\right| \leqq \sqrt{|D|}.$$

Wegen $|B| < \sqrt{|D|}$ muß also auch

$$\left|2C\frac{X}{Y}\right| \leqq \sqrt{|D|} \quad \text{oder} \quad |C^2X^2| \leqq |ACY^2|$$

sein, oder

$$|CX^2| \leqq |AY^2|.$$

Wir haben also: Für

(6) $$|CX^2| \leqq |AY^2| \quad \text{gilt} \quad |N\alpha| = |(2CX+BY)^2 - DY^2| = |ACY^2|.$$

Die Gleichungen (5), (6) ergeben für $Z(s, \mathfrak{R})$ (nach (4)):

(7) $$Z(s,\mathfrak{R}) = \frac{1}{w\cdot|C|^s}\cdot\sum_{\substack{|CX^2|\\ >|AY^2|}}\frac{1}{|X|^{2s}} + \frac{1}{w|A|^s}\cdot\sum_{\substack{|CX^2|\\ \leqq|AY^2|}}\frac{1}{|Y|^{2s}}.$$

Diese beiden Summen können nun jede für sich summiert werden. Wir setzen

$$|A| = p^a, \quad |C| = p^b.$$

Dann ist wegen $|AC| = |D|$ und $|C| \leqq \sqrt{D}$, $a - b \geqq 0$. Wir setzen weiter: $r = \left[\frac{a-b}{2}\right]$, wo $[\,]$ die nächstkleinere ganze Zahl bedeutet.

I. In der ersten Summe halten wir zunächst Y fest.

Für $Y = 0$ ist einfach über alle $X \neq 0$ zu summieren. Dies gibt als Beitrag (vom Grade ν gibt es $(p-1)p^\nu$ Funktionen):

$$\frac{1}{w|C|^s} \cdot \sum_{\nu=0}^{\infty} \frac{(p-1)p^\nu}{p^{2\nu s}} = \frac{p-1}{w|C|^s} \cdot \frac{1}{1-p^{-(2s-1)}}.$$

Für $|Y| = p^\mu$ ist über jene Werte von X zu summieren, für die $|X| > p^{\frac{a-b}{2}+\mu}$ ist, also, $|X| = p^\nu$ gesetzt, für die $\nu > \frac{a-b}{2} + \mu$, oder schließlich $\nu > r + \mu$ ist. Dies gibt als Beitrag:

$$\frac{1}{w|C|^s} \cdot \sum_{\nu=r+\mu+1}^{\infty} \frac{(p-1)p^\nu}{p^{2\nu s}} = \frac{p-1}{w|C|^s} \cdot \frac{p^{-(r+\mu+1)(2s-1)}}{1-p^{-(2s-1)}}.$$

Wird nun über alle $Y \neq 0$, d. h. über alle μ (wobei jedes μ genau $(p-1)p^\mu$-mal zu berücksichtigen ist) summiert, so erhält man:

$$\frac{p-1}{w|C|^s} \cdot \frac{p^{-(r+1)(2s-1)}}{1-p^{-(2s-1)}} \cdot \sum_{\mu=0}^{\infty} (p-1)p^\mu \cdot p^{-\mu(2s-1)}$$

$$= \frac{(p-1)^2}{w|C|^s} \frac{p^{-(r+1)(2s-1)}}{(1-p^{-(2s-1)})} \cdot \sum_{\mu=0}^{\infty} p^{-2\mu(s-1)} = \frac{(p-1)^2}{w|C|^s} \cdot \frac{p^{-(r+1)(2s-1)}}{1-p^{-(2s-1)}} \cdot \frac{1}{1-p^{-2(s-1)}}.$$

Die erste Summe hat also den Wert

$$\frac{p-1}{w|C|^s} \cdot \frac{1}{1-p^{-(2s-1)}} + \frac{(p-1)^2}{w|C|^s} \cdot \frac{p^{-(r+1)(2s-1)}}{(1-p^{-(2s-1)})(1-p^{-2(s-1)})}.$$

II. In der zweiten Summe werde X festgehalten. Für $X = 0$ ist über alle $Y \neq 0$ zu summieren, was liefert:

$$\frac{1}{w|A|^s} \cdot \sum_{\nu=0}^{\infty} \frac{(p-1)p^\nu}{p^{2\nu s}} = \frac{p-1}{w|A|^s} \cdot \frac{1}{1-p^{-(2s-1)}}.$$

Für $|X| = p^\mu$ soll nun $|Y| = p^\nu \geqq p^{\frac{b-a}{2}+\mu}$ sein oder $\nu \geqq \frac{b-a}{2} + \mu$, also $\nu \geqq \mu - r$. Außerdem soll natürlich, da Y ganz ist, ν nicht negativ sein. Solange nun $\mu < r$ ist, ist einfach über alle $Y \neq 0$ zu summieren. Dies liefert für jedes X:

$$\frac{p-1}{w|A|^s} \cdot \sum_{\nu=0}^{\infty} \frac{p^\nu}{p^{2\nu s}} = \frac{p-1}{w|A|^s} \cdot \frac{1}{1-p^{-(2s-1)}}.$$

Im ganzen also, wenn über alle in Betracht kommenden X, das ist für $\mu < r$, summiert wird:

$$\frac{p-1}{w\,|A|^s}\,\frac{1}{1-p^{-(2s-1)}}\cdot\sum_{\mu=0}^{r-1}(p-1)\,p^{\mu}=\frac{(p-1)^2}{w\,|A|^s}\,\frac{p^r-1}{p-1}\,\frac{1}{1-p^{-(2s-1)}}.$$

Die beiden bis jetzt behandelten Beiträge geben zusammen

$$\frac{p-1}{w\,|A|^s}\cdot\frac{p^r}{1-p^{-(2s-1)}}.$$

Für $\mu \geqq r$ ist aber $\nu \geqq \mu - r$, also ν nicht negativ. Dies gibt

$$\frac{1}{w\,|A|^s}\sum_{\nu=\mu-r}^{\infty}\frac{(p-1)\,p^{\nu}}{p^{2\nu s}}=\frac{p-1}{w\,|A|^s}\cdot\frac{p^{-(\mu-r)(2s-1)}}{1-p^{-(2s-1)}}.$$

Wird dies über alle in Betracht kommenden X, also über $\mu \geqq r$ summiert, so erhalten wir:

$$\frac{p-1}{w\,|A|^s}\cdot\frac{p^{r(2s-1)}}{1-p^{-(2s-1)}}\cdot\sum_{\mu=r}^{\infty}p^{-\mu(2s-1)}\cdot(p-1)\,p^{\mu}$$

$$=\frac{(p-1)^2}{w\,|A|^s}\cdot\frac{p^{r(2s-1)}}{1-p^{-(2s-1)}}\cdot\frac{p^{-2r(s-1)}}{1-p^{-2(s-1)}}=\frac{(p-1)^2}{w\,|A|^s}\cdot\frac{p^r}{(1-p^{-(2s-1)})\,(1-p^{-2(s-1)})}.$$

Der Wert der zweiten Summe ist also:

$$\frac{p-1}{w\,|A|^s}\cdot\frac{p^r}{1-p^{-(2s-1)}}+\frac{(p-1)^2}{w\,|A|^s}\cdot\frac{p^r}{(1-p^{-(2s-1)})\,(1-p^{-2(s-1)})}.$$

Dies gibt für $Z(s,\mathfrak{K})$:

$$(8)\qquad Z(s,\mathfrak{K})=\left(\frac{p^r}{|A|^s}+\frac{1}{|C|^s}\right)\frac{p-1}{w\,(1-p^{-(2s-1)})}$$

$$+\left(\frac{p^{-(r+1)(2s-1)}}{|C|^s}+\frac{p^r}{|A|^s}\right)\frac{(p-1)^2}{w\,(1-p^{-(2s-1)})\,(1-p^{-2(s-1)})}.$$

Aus (8) folgt für $s=0$

$$Z(0,\mathfrak{K})=(p^r+1)\cdot\frac{p-1}{w\,(1-p)}+\frac{(p-1)^2}{w\,(1-p)\,(1-p^2)}\,(p^{r+1}+p^r)$$

$$=-\frac{p^r+1}{w}+\frac{p^r}{w},$$

also

$$(9)\qquad Z(0,\mathfrak{K})=-\frac{1}{w}.$$

Aus § 17, (13) folgt also

$$Z(0)=\sum_{\mathfrak{K}}Z(0,\mathfrak{K})=-\frac{h}{w},\quad\text{wo } h \text{ die Klassenzahl ist,}$$

also

$$h=-wZ(0).$$

Für $D = g$ ist $w = p^2 - 1$, so daß § 17, (11) den bekannten Wert $h = 1$ wiedergibt. Der triviale Fall $D = g$ werde nun künftighin stets ausgeschlossen. Dann ist $w = p - 1$, und § 17, (9) gibt

$$h = \sum_{\nu=0}^{n-1} \sigma_\nu = \sigma_0 + \sigma_1 + \sigma_2 + \ldots + \sigma_{n-1}. \tag{10}$$

Dies ist, da h der Bedeutung nach stets positiv ist, die Ergänzung zu § 17, (7).

Einen anderen, weniger einfachen Ausdruck für h erhalten wir aus den Residuen für $s = 1$. Es ist nämlich

$$\lim_{s=1} (s-1)\, Z(s, \mathfrak{K}) = \frac{(p-1)^2}{w\left(1 - \frac{1}{p}\right) 2 \log p} \cdot \left(\frac{p^{-r-1}}{|C|} + \frac{p^r}{|A|}\right).$$

1. Nochmals $D = g$: Hier ist also $|C| = 1$ und $|A| = 1$, $r = 0$, $w = p^2 - 1$, somit

$$\lim_{s=1} (s-1)\, Z(s, \mathfrak{K}) = \frac{p}{2(p+1)\log p} \cdot (p^{-1} + 1) = \frac{1}{2 \log p}.$$

Also gibt § 17 (11) wieder $h = 1$.

2. Grad von D ungerade: Aus $|AC| = |D|$ folgt, daß $a + b$, also auch $a - b$ ungerade und demnach $r = \frac{a-b}{2} - \frac{1}{2}$ ist. Also:

$$p^r = p^{\frac{a-b}{2} - \frac{1}{2}} = \frac{1}{\sqrt{p}} \sqrt{\left|\frac{A}{C}\right|}.$$

Somit

$$\lim_{s=1} (s-1)\, Z(s, \mathfrak{K}) = \frac{p}{2 \log p} \cdot \left(\frac{1}{\sqrt{p}} \cdot \frac{1}{\sqrt{|AC|}} + \frac{1}{\sqrt{p}} \cdot \frac{1}{\sqrt{|AC|}}\right) = \frac{\sqrt{p}}{\sqrt{|D|} \log p}.$$

Das Residuum ist also von der Klasse unabhängig und somit

$$\lim_{s=1} (s-1)\, Z(s) = \frac{\sqrt{p} \cdot h}{\sqrt{|D|} \cdot \log p}.$$

Wegen § 17, (10) ist

$$h = \sqrt{\frac{|D|}{p}} \cdot \sum_{\nu=0}^{n-1} \frac{\sigma_\nu}{p^\nu}. \tag{11}$$

3. Grad von D gerade: Dann ist $r = \frac{a-b}{2}$, also $p^r = \sqrt{\left|\frac{A}{C}\right|}$;

$$\lim_{s=1} (s-1)\, Z(s, \mathfrak{K}) = \frac{p}{2 \log p} \left(\frac{1}{p} \cdot \frac{1}{\sqrt{|AC|}} + \frac{1}{\sqrt{|AC|}}\right) = \frac{(p+1)}{2\sqrt{|D|} \cdot \log p},$$

also

$$\lim_{s=1} Z(s) = \frac{(p+1)h}{2\sqrt{|D|} \cdot \log p}$$

und

$$h = \frac{2\sqrt{|D|}}{p+1} \cdot \sum_{\nu=0}^{n-1} \frac{\sigma_\nu}{p^\nu} \,. \tag{11a}$$

Die Beziehung zwischen (10) und (11), (11a) werden wir später erkennen. Für die Zetafunktion hat unsere Residuenbildung die Erkenntnis zur Folge, daß die Stellen $s = 1 + \frac{2k\pi i}{\log p}$ wirklich Pole erster Ordnung sind.

§ 13.

Die Anzahl der Idealklassen im reellen Körper.

Es sei $K(\sqrt{D})$ ein reeller Körper, $\varepsilon_0 = U + V\sqrt{D}$ seine Grundeinheit. Dann ist $V \neq 0$ und $|\varepsilon_0| > 1$, sowie $|\varepsilon_0'| = |U - V\sqrt{D}| < 1$. In ε_0' müssen sich also die höchsten Potenzen heben, so daß sie sich in ε_0 nicht heben können. Es ist also

$$\varepsilon_0 = V\sqrt{D} \geqq \sqrt{D} \,.$$

Sei nun α eine ganze Funktion des Körpers. Wir betrachten die Lage von $|\alpha|$ in der Intervallfolge

$$\ldots, \quad |\varepsilon_0|^{-2}, \quad |\varepsilon_0|^{-1}, \quad 1, \quad |\varepsilon_0|, \quad |\varepsilon_0|^2, \quad \ldots$$

Dann muß es ein und nur ein ν geben, so daß

$$|\varepsilon_0^{\nu+1}| \leqq |\alpha| < |\varepsilon_0^{\nu+2}|, \quad \text{also} \quad |\varepsilon_0| \leqq |\alpha \varepsilon_0^{-\nu}| < |\varepsilon_0|^2 .$$

Da nun α mit $\alpha\varepsilon_0^{-\nu}$ assoziiert ist, gibt es zu jeder Funktion eine mit ihr assoziierte, die jetzt mit α bezeichnet werde, für die $|\varepsilon_0| \leqq |\alpha| < |\varepsilon_0|^2$, und zwar gibt es zu jeder Funktion genau $p - 1$ assoziierte, welche diese Bedingung befriedigen, nämlich die Funktionen $a\alpha$ $(a = 1, 2, 3, \ldots, p-1)$. Die Beträge der Normen dieser $p - 1$ Funktionen sind alle dieselben. Aus § 17, (14) folgt also

$$Z(s, \mathfrak{R}) = \frac{|N\mathfrak{a}|^s}{p-1} \cdot \sum_{\alpha \equiv 0 \,(\mathrm{mod}\,\mathfrak{a})}{}' \frac{1}{|N\alpha|^s} \,, \tag{1}$$

mit der Nebenbedingung

$$|\varepsilon_0| \leqq |\alpha| < |\varepsilon_0|^2 . \tag{2}$$

Für das Ideal $\mathfrak{a}$ wählen wir nun wieder ein reduziertes Ideal aus $\mathfrak{R}$ mit der Basis $\mathfrak{a} = (2C, B + \sqrt{D})$. Dann ist bekanntlich

$$|B - \sqrt{D}| < |C| < |B + \sqrt{D}| = |B| = |\sqrt{D}| \quad \text{und} \quad |N\mathfrak{a}| = |C| . \tag{3}$$

In (1) ist also zu setzen $\alpha = 2CX + (B - \sqrt{D})Y$ und unter Beachtung von (2) über alle X, Y zu summieren.

Für unsere Zwecke genügt es nun, $\lim_{s=1}(s-1)Z(s,\mathfrak{K})$ zu bilden. Dabei kommt es ersichtlich nicht auf endlich viele Glieder der Summe an.

Diskussion von (2) und (3):

I. Sei

$$|2CX| > |B-\sqrt{D}|\cdot|Y|.$$

Dann ist $|\alpha| = |CX|$, und (2) ergibt

$$\varepsilon_0 \leqq |CX| < |\varepsilon_0|^2.$$

Dies kann nur für endlich viele X eintreten. Zu jedem solchen X soll nun $|B+\sqrt{D}|\cdot|Y| < |2C\mathfrak{X}|$ sein. Dies liefert auch nur endlich viele Y. Unsere Annahme gibt also nur endlich viele Glieder der Summe.

II. Sei

$$|2CX| < |B+\sqrt{D}|\cdot|Y|.$$

Dann ist $|\alpha| = |(B+\sqrt{D})Y|$ und nach (2)

$$\varepsilon_0 \leqq |(B-\sqrt{D})Y| < |\varepsilon_0|^2.$$

Auch dieser Fall kann nur für endlich viele Y und endlich viele X zutreffen, liefert also auch nur endlich viele Glieder.

III. Sei

$$|2CX| = |(B+\sqrt{D})Y|.$$

Dann ist also wegen (3) sicher

$$|2CX| \geqq |(B+\sqrt{D})Y|,$$

also

$$|\alpha'| = |2CX+(B-\sqrt{D})Y| = |CX|. \tag{4}$$

Aus

$$|\varepsilon_0| \leqq |2CX-(B+\sqrt{D})Y| < |\varepsilon_0|^2$$

folgt wegen $|B+\sqrt{D}| = |\sqrt{D}|$

$$\frac{|\varepsilon_0|}{|\sqrt{D}|} \leqq \left|\frac{2CX}{B+\sqrt{D}}+Y\right| < \frac{|\varepsilon_0|^2}{|\sqrt{D}|}. \tag{5}$$

Wegen III. gibt es nun zu jedem X nur endlich viele Y. Es gibt also nur endlich viele Glieder der Summe, für die $\left|\frac{2CX}{B+\sqrt{D}}\right| \leqq \frac{|\varepsilon_0|^2}{|\sqrt{D}|}$ ist. Wir können also annehmen, es sei

$$\left|\frac{2CX}{B+\sqrt{D}}\right| > \frac{|\varepsilon_0|^2}{|\sqrt{D}|}. \tag{6}$$

Am Anfang dieses Paragraphen zeigten wir nun $\frac{|\varepsilon_0|}{|\sqrt{D}|} \geqq 1$. Der

mittlere Teil von (5) hat also sicher keinen negativen Grad. Wir können also alle negativen Potenzen weglassen, so daß (5) gleichbedeutend ist mit

$$\frac{|\varepsilon_0|}{|\sqrt{D}|} \leqq E\left(\frac{2CX}{B+\sqrt{D}}\right) + Y < \frac{|\varepsilon_0|^2}{|\sqrt{D}|}.$$

(Über E siehe § 10.) Setzen wir also

$$Y = -E\left(\frac{2CX}{B+\sqrt{D}}\right) + F \qquad (F \text{ ganz}), \tag{7}$$

so muß gelten

$$\frac{|\varepsilon_0|}{|\sqrt{D}|} \leqq |F| < \frac{|\varepsilon_0|^2}{|\sqrt{D}|}. \tag{8}$$

Sei umgekehrt (8) erfüllt und Y durch (7) bestimmt. Wegen (6) gilt erst recht

$$\left|\frac{2CX}{B+\sqrt{D}}\right| > |F|, \quad \text{also} \quad |Y| = \left|\frac{2CX}{B+\sqrt{D}}\right|,$$

somit

$$|2CX| = |(B+\sqrt{D})\cdot Y|.$$

Dies ist also Bedingung III. Daß (5) erfüllt ist, folgt aus (7) und (8) unmittelbar.

Wir haben also für alle (6) genügenden X für Y (7) zu setzen, wo F der Bedingung (8) genügt, und über alle in Betracht kommenden X und F zu summieren. Nun ist aber wegen (7) und (8)

$$\alpha = |2CX + (B+\sqrt{D})Y| = |\sqrt{D}|\cdot\left|\frac{2CX}{B+\sqrt{D}} + Y\right| = |\sqrt{D}|\cdot|F|,$$

und nach (4)

$$|\alpha'| = |CX|.$$

Also ist

$$N\alpha = \alpha\alpha' = |C\sqrt{D}|\cdot|XF|.$$

Statt nun über alle X, welche (6) genügen, zu summieren, können wir über alle X überhaupt summieren, wenn nur erneut das Resultat um endlich viele Glieder korrigiert wird.

Wegen (1) ist also

$$Z(s, \mathfrak{K}) = \frac{|C|^s}{p-1}\cdot\sum_X{}'\sum_F{}'\frac{1}{|C\sqrt{D}XF|^s} + G,$$

wo über alle X und über alle (8) genügenden F zu summieren ist, und G eine endliche Anzahl Glieder bedeutet.

Somit ist

$$Z(s, \mathfrak{K}) = \frac{1}{(p-1)\,|\sqrt{D}|^s}\cdot\left(\sum_X{}'\frac{1}{|X|^s}\right)\cdot\left(\sum_F{}'\frac{1}{|F|^s}\right) + G.$$

Setzen wir nun

$$|\varepsilon_0| = p^R, \quad \text{also} \quad R = \frac{\log|\varepsilon_0|}{\log p}, \tag{9}$$

so daß R die Rolle des „Regulators“ übernimmt und jedenfalls positiv ganz ist, ferner

$$|\sqrt{D}| = p^{\frac{n}{2}}, \quad \text{wo } \frac{n}{2} \text{ ganz ist,}$$

da ein reeller Körper vorliegt, so wird

$$Z(s,\mathfrak{K}) = \frac{1}{(p-1)|\sqrt{D}|^s} \cdot \sum_{\nu=0}^{\infty}{}' \frac{(p-1)p^\nu}{p^{\nu s}} \cdot \sum_{\mu=(R-\frac{n}{2})}^{(2R-\frac{n}{2}-1)}{}' \frac{(p-1)p^\mu}{p^{\mu s}} + G \tag{10}$$

$$= \frac{p-1}{|\sqrt{D}|^s(1-p^{-(s-1)})} \cdot \frac{1-p^{-R(s-1)}}{1-p^{-(s-1)}} \cdot p^{-(R-\frac{n}{2})(s-1)} + G.$$

Da G nur aus endlich viel Gliedern besteht, ist $\lim_{s=1}(s-1)G = 0$. Demnach finden wir

$$\lim_{s=1}(s-1)Z(s,\mathfrak{K}) = \frac{(p-1)R}{|\sqrt{D}|\cdot\log p}, \tag{11}$$

also ein von der Klasse unabhängiges Residuum. Es ergibt also § 17, (13), (10):

$$\lim_{s=1}(s-1)Z(s) = \frac{(p-1)Rh}{|\sqrt{D}|\log p}, \tag{12}$$

$$h = \frac{|\sqrt{D}|}{(p-1)R} \cdot \sum_{\nu=0}^{n-1}{}' \frac{\sigma_\nu}{p^\nu}. \tag{13}$$

Die Zetafunktion hat also auch hier in $s = 1 + \frac{2k\pi i}{\log p}$ Pole erster Ordnung.

§ 20.

Das Nichtverschwinden von $Z(s)$ auf der Geraden $\Re(s) = 1$.

Setzen wir

$$\varkappa = \begin{cases} \frac{2\sqrt{|D|}}{p+1}, & \text{falls Grad von } D \text{ gerade} \\ \sqrt{\frac{|D|}{p}}, & \text{falls Grad von } D \text{ ungerade} \end{cases} \Big\} \text{ Körper imaginär,} \tag{1}$$

$$\frac{|\sqrt{D}|}{(p-1)R}, \text{ falls Grad von } D \text{ gerade, Körper reell,}$$

so ist

$$\lim_{s=1}(s-1)Z(s) = \frac{h}{\varkappa\log p} \neq 0. \tag{2}$$

Die Pole erster Ordnung sind die Stellen $s = 1 + \frac{2k\pi i}{\log p}$. Sonst ist $Z(s)$ überall regulär. Die Produktdarstellung § 17, (1) lehrt, daß $Z(s)$ in der Halbebene $\Re(s) > 1$ keine Nullstellen besitzt. Wir wollen zeigen, daß auch auf $\Re(s) = 1$ keine Nullstelle liegt.

Satz. Die Stellen $s = 1 + \frac{(2k+1)\pi i}{\log p}$ sind keine Nullstellen von $Z(s)$.

Beweis. Da $Z(s)$ periodisch mit der Periode $\frac{2\pi i}{\log p}$ ist, genügt der Nachweis für $s = 1 + \frac{\pi i}{\log p}$. Aus § 17, (8) folgt nun

$$\lim_{s=1} Z_D\left(s + \frac{\pi i}{\log p}\right) = \frac{1}{2} \lim_{s=1} \frac{1 - p^{-(s-1)}}{s-1} \cdot \lim_{s=1} (s-1)\, Z_{gD}(s).$$

Bezeichnet man also mit h' und $\varkappa'$ die Größen des Körpers $K(\sqrt{gD})$, so ist

$$Z_D\left(1 + \frac{\pi i}{\log p}\right) = \frac{h'}{2\varkappa'} \neq 0,$$

q. e. d.

Satz. $Z(s)$ hat auf der Geraden $\Re(s) = 1$ keine Nullstelle.

Beweis. Nach dem soeben Gezeigten dürfen wir die Stellen $s = 1 + \frac{k\pi i}{\log p}$ ausschließen.

Wir setzen $s = \sigma + it$. (Der Buchstabe t hat natürlich nichts mit unserem Adjunktionsbuchstaben t zu tun; ich wähle diese Bezeichnung nur, um den Anschluß an die üblichen Beweise zu haben.)

Nach § 17 ist dann

$$Z(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{N\mathfrak{p}^s}} \quad \text{für} \quad \Re(s) > 1.$$

Daraus folgt wie bekannt

$$-\frac{Z'(s)}{Z(s)} = \sum_{\mathfrak{p},\mathfrak{m}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}^{ms}}.$$

Sei nun $1 + t_0 i$ eine Nullstelle k-ter Ordnung $(k \geqq 1)$, wobei $t_0 \neq \frac{\nu\pi}{\log p}$. Dann ist $1 + 2t_0 i$ sicher kein Pol. Es ist also eine Nullstelle l-ter Ordnung mit $l \geqq 0$.

Der weitere Beweis verläuft so vollständig analog dem gewöhnlichen, daß seine weitere Ausführung unterdrückt werden darf. Ich verweise etwa auf Landau, Theorie der algebraischen Zahlen und Ideale, Seite 101. Wie dort findet man

$$k \leqq \frac{3-l}{4}, \quad \text{also wegen } l \geqq 0, \quad k \leqq \frac{3}{4} \quad \text{entgegen} \quad k \geqq 1.$$

Satz. Die obere Grenze θ der reellen Teile der Nullstelle von $Z(s)$ ist kleiner als eins $\theta < 1$.

Beweis. Für $\Re(s) \geqq 1$ besitzt $Z(s)$ keine Nullstelle. Da $Z(s)$ aber die rein imaginäre Periode $\frac{2\pi i}{\log p}$ hat, können wir schließen, daß die obere Grenze der reellen Teile der Nullstellen von $Z(s)$ kleiner als eins ist.

§ 21.

Die Funktionalgleichung von $Z(s)$ und die Relationen zwischen den σ_ν.

Wir kehren zur Formel (8) des § 18 zurück und diskutieren die verschiedenen, für imaginäre Körper sich ergebenden Fälle.

1. $|D| = p^{2m+1}$. Wir setzen $|A| = p^\nu$. Wegen $D = AC$ wird

$$|C| = p^{2m-\nu+1}, \quad \text{also} \quad r = \left[\frac{\nu-(2m-\nu+1)}{2}\right] = \nu - m - 1, \quad w = p-1.$$

Wir haben dann

$$Z(s,\Re) = \left(\frac{p^{\nu-m-1}}{p^{\nu s}} + \frac{1}{p^{(2m-\nu+1)s}}\right)\frac{1}{1-p^{-(2s-1)}}$$

$$+ \frac{p-1}{(1-p^{-(2s-1)})(1-p^{-2(s-1)})}\cdot\left(\frac{p^{-(\nu-m)(2s-1)}}{p^{(2m-\nu+1)s}} + \frac{p^{\nu-m-1}}{p^{\nu s}}\right) = \frac{p^{\nu-m-1} + p^{(2\nu-2m-1)s}}{p^{\nu s}(1-p^{-(2s-1)})}$$

$$+ \frac{(p-1)\cdot p^{\nu-m-1}}{(1-p^{-(2s-1)})(1-p^{-(s-1)})(1+p^{-(s-1)})}\cdot\frac{1}{p^{\nu s}}(p^{-(s-1)}+1).$$

$$Z(s,\Re) = \frac{p^{\nu-m-1}+p^{(2\nu-2m-1)s}}{p^{\nu s}(1-p^{-(2s-1)})} + \frac{(p-1)p^{\nu-m-1}}{p^{\nu s}(1-p^{-(2s-1)})(1-p^{-(s-1)})}$$

$$= \frac{p^{\nu-m-1}+p^{(2\nu-2m-1)s}-p^{\nu-m-1}p^{-(s-1)}-p\cdot p^{2(\nu-m-1)s}\cdot p^{\nu-m}\ p^{\nu-m-1}}{p^{\nu s}(1-p^{-(2s-1)})(1-p^{-(s-1)})}.$$

$$Z(s,\Re) = \frac{p^{(2\nu-2m-1)s}-p^{\nu-m}\cdot p^{-s}-p\cdot p^{2(\nu-m-1)s}+p^{\nu-m}}{p^{\nu s}(1-p^{-(2s-1)})(1-p^{-(s-1)})}.$$

Daraus ersieht man unmittelbar, daß $Z(s,\Re)$ in $s=\frac{1}{2}$ keinen Pol hat. Es ist also überall bis auf die Pole $s = 1 + \frac{2k\pi i}{\log p}$ regulär.

Ferner ist

$$Z(1-s,\Re) = \frac{p^{(2\nu-2m-1)(1-s)}-p^{\nu-m-1}\cdot p^{s}-p\cdot p^{2(\nu-m-1)(1-s)}+p^{\nu-m}}{p^{\nu(1-s)}(1-p^{2s-1})(1-p^{s})}.$$

Erweitern wir den Bruch mit $p^{(\nu-m-1)(2s-1)}$, so wird

$$Z(1-s,\Re) = \frac{p^{\nu-m}\cdot p^{-s}-p^{(2\nu-2m-1)s}-p^{\nu-m}+p\cdot p^{2(\nu-m-1)s}}{p^{\nu s}\cdot p^{-m(2s-1)}(p^{-(2s-1)}-1)(1-p^{s})}$$

$$= p^{m(2s-1)}\cdot\frac{1-p^{-(s-1)}}{1-p^{s}}\cdot Z(s,\Re).$$

Demnach haben wir die Funktionalgleichung

$$(1) \qquad Z(1-s,\mathfrak{K}) = \frac{1-p^{-(s-1)}}{1-p^{s}} \cdot \left(\sqrt{\frac{|D|}{p}}\right)^{2s-1} Z(s,\mathfrak{K}).$$

2. $|D| = p^{2m}$. $|A| = p^{\nu}$ also $|C| = p^{2m-\nu}$; $r = \nu - m$.

$$Z(s,\mathfrak{K}) = \left(\frac{p^{\nu-m}}{p^{\nu s}} + \frac{1}{p^{(2m-\nu)s}}\right) \cdot \frac{1}{1-p^{-(2s-1)}}$$

$$\cdot \frac{(p-1)}{(1-p^{-(2s-1)})(1-p^{-2(s-1)})} \cdot \left(\frac{p^{-(\nu-m+1)(2s-1)}}{p^{(2m-\nu)s}} + \frac{p^{\nu-m}}{p^{\nu s}}\right)$$

$$= \frac{p^{\nu-m} + p^{2(\nu-m)s}}{p^{\nu s}(1-p^{-(2s-1)})} + \frac{(p-1)p^{\nu-m}(1+p^{(2s-1)})}{p^{\nu s}(1-p^{-(2s-1)})(1-p^{-2(s-1)})}$$

$$+p^{2(\nu-m)s} - p^{\nu-m}\cdot p^{-2(s-1)} - p^{2}p^{2(\nu-m-1)s} + p^{\nu-m-1} + p^{\nu-m+1}\cdot p^{-(2s-1)} - p^{\nu-m} - p^{\nu-m}\cdot p^{-(2s-1)}$$

$$= \frac{p^{2(\nu-m)s} - p^{2}p^{2(\nu-m-1)s} + p^{\nu-m+1} - p^{\nu-m+1}\cdot p^{-2s}}{p^{\nu s}(1-p^{-(2s-1)})(1-p^{-2(s-1)})}.$$

Daraus ersieht man wieder die Regularität für $s = \frac{1}{2}$. $Z(s,\mathfrak{K})$ ist überall regulär bis auf die Pole $s = 1 + \frac{k\pi i}{\log p}$. Ferner ist

$$Z(1-s,\mathfrak{K}) = \frac{p^{2(\nu-m)}\cdot p^{-2(\nu-m)s} - p^{2(\nu-m)}\cdot p^{-2(\nu-m-1)s} + p^{\nu-m+1} - p^{\nu-m-1}\cdot p^{2s}}{p^{\nu(1-s)}(1-p^{2s-1})(1-p^{2s})}.$$

Erweitern wir mit $p^{-(\nu-m-1)}\cdot p^{2(\nu-m-1)s}$, so wird

$$Z(1-s,\mathfrak{K}) = \frac{p^{\nu-m+1}\cdot p^{-2s} - p^{\nu-m+1} + p^{2}p^{2(\nu-m-1)s} - p^{2(\nu-m)s}}{p^{\nu s}\cdot p^{-m(2s-1)}(p^{-(2s-1)}-1)(1-p^{2s})}$$

$$= p^{m(2s-1)}\cdot\frac{1-p^{-2(s-1)}}{1-p^{2s}}\cdot Z(s,\mathfrak{K}).$$

Demnach lautet die Funktionalgleichung

$$(2) \qquad Z(1-s,\mathfrak{K}) = \frac{1-p^{-2(s-1)}}{1-p^{2s}}(\sqrt{|D|})^{2s-1} Z(s,\mathfrak{K}).$$

Summation über alle Klassen liefert die gesuchte Funktionalgleichung für die Zetafunktion:

$$(3) \qquad Z(1-s) = \frac{1-p^{-(s-1)}}{1-p^{s}}\left(\sqrt{\frac{|D|}{p}}\right)^{2s-1} Z(s),$$

falls Grad von D ungerade,

$$(4) \qquad Z(1-s) = \frac{1-p^{-2(s-1)}}{1-p^{2s}}(\sqrt{D})^{2s-1} Z(s),$$

falls Grad von D gerade, Körper imaginär.

Um auch für reelle Körper die Funktionalgleichung zu gewinnen, gehen wir aus von § 17, (8):

$$Z_D\left(s+\frac{\pi i}{\log p}\right)=\frac{1-p^{-(s-1)}}{1+p^{-(s-1)}}Z_{gD}(s). \tag{5}$$

Wenn nun $K(\sqrt{g}D)$ reell ist, steht links der Zetafunktion des imaginären Körpers $K(\sqrt{D})$, welche die Funktionalgleichung (4) hat. Ersetzt man also in (4) s durch $s+\frac{\pi i}{\log p}$ und berücksichtigt (5) und die Periodizität von $Z(s)$ und p^s, so erhält man, wenn $Z(s)$ jetzt die Zetafunktion des reellen Körpers ist:

$$\frac{1-p^s}{1+p^s}Z(1-s)=\frac{1-p^{-2(s-1)}}{1-p^{2s}}\cdot\frac{1-p^{-(s-1)}}{1+p^{-(s-1)}}\cdot(\sqrt{|D|})^{2s-1}\cdot Z(s).$$

Demnach, falls Körper reell, das Resultat

$$Z(1-s)=\left(\frac{1-p^{-(s-1)}}{1-p^s}\right)^2(\sqrt{|D|})^{2s-1}Z(s). \tag{6}$$

Aus der Funktionalgleichung folgt, da $Z(s)$ für $\Re(s)\geqq 1$ keine Nullstelle besitzt und die Pole erster Ordnung $1-\frac{2k\pi i}{\log p}$ hat, nach einfacher Diskussion:

In der Halbebene $\Re(s)<0$ liegt keine Nullstelle von $Z(s)$.

1. Grad von D ungerade. $Z(s)$ hat auch auf der Geraden $\Re(s)=0$ keine Nullstelle.

2. Grad von D gerade, Körper imaginär. Auf $\Re(s)=0$ liegen nur die Nullstellen erster Ordnung: $s=\frac{(2k+1)\pi i}{\log p}$.

3. Grad von D gerade, Körper reell. Auf $\Re(s)=0$ liegen nur die Nullstellen erster Ordnung: $s=\frac{2k\pi i}{\log p}$.

Alle übrigen „nicht trivialen" Nullstellen gehören dem Streifen $0<1-\theta\leqq\Re(s)\leqq\theta<1$ an, wo θ die obere Grenze ihrer reellen Teile ist. Sie liegen symmetrisch zur Geraden $\Re(s)=\frac{1}{2}$ und zur reellen Achse.

Beim reellen Körper ist also $s=0$ Nullstelle erster Ordnung. Wir verwenden die Funktionalgleichung (6) dazu, eine elegantere Formel für die Klassenzahl des reellen Körpers zu gewinnen. Es folgt nämlich aus (6), da $Z(0)=0$ ist, nach § 20, (1), (2):

$$Z'(0)=\lim_{s=0}\frac{Z(s)}{s}=\lim_{s=0}\left[\left(\frac{1-p^s}{s}\right)^2\cdot\frac{(\sqrt{|D|})^{1-2s}}{(1-p^{-(s-1)})^2}\right]\cdot\lim s\cdot Z(1-s)$$

$$=\frac{(\log p)^2}{(p-1)^2}\cdot\sqrt{|D|}\cdot\lim_{s_1=1}(s_1-1)Z(s_1)=\frac{(\log p)^2}{(p-1)^2}\sqrt{|D|}\cdot\frac{h}{\varkappa\log p}$$

$$\frac{hR}{p-1}\cdot\log p.$$

Also

$$h = -\frac{p-1}{R \log p} \cdot Z'(0).$$

Setzt man nun

$$L(s) = (1 - p^{-(s-1)}) Z(s) = \sum_{\nu=0}^{n-1}{}' \frac{\sigma_\nu}{p^{\nu s}},$$

so folgt aus $Z(0) = 0$:

$$L'(0) = (1-p) Z'(0) = -\sum_{\nu=0}^{n-1}{}' \nu \sigma_\nu \log p.$$

Also ist

$$h = \frac{1}{R \log p} L'(0) = -\frac{1}{R} \sum_{\nu=1}^{n-1}{}' \nu \sigma_\nu.$$

Für reelle Körper haben wir also die Formel

$$(7) \quad h = -\frac{1}{R} \sum_{\nu=1}^{n-1}{}' \nu \sigma_\nu = -\frac{1}{R} (\sigma_1 + 2\sigma_2 + 3\sigma_3 + \ldots + (n-1)\sigma_{n-1}),$$

wo $R = \frac{\log |\varepsilon_0|}{\log p}$ der Regulator von $K(\sqrt{D})$ ist.

Die Funktionalgleichung hat nun merkwürdige Relationen zwischen den Zahlen σ_ν zur Folge, welche zum Beispiel die Berechnung der Klassenzahl sehr vereinfachen und die Beziehung zwischen unseren beiden Arten von Klassenzahlformeln aufdecken:

1. Grad von D ungerade: $D = p^{2m+1}$. Aus (3) folgt, daß die Funktion

$$(8) \quad \Xi(s) = (1 - p^{-(s-1)}) \left(\sqrt{\frac{D}{p}}\right)^{s-\frac{1}{2}} Z(s) = p^{m(s-\frac{1}{2})} \sum_{\nu=0}^{2m}{}' \frac{\sigma_\nu}{p^{\nu s}}$$

$$= \sum_{\nu=0}^{2m}{}' \sigma_\nu \cdot p^{-\frac{m}{2}} \cdot p^{(m-\nu)s}$$

der Funktionalgleichung genügt:

$$(9) \quad \Xi(1-s) = \Xi(s).$$

Nun ist

$$\Xi(1-s) = \sum_{\nu=0}^{2m}{}' \sigma_\nu p^{-\frac{m}{2}} \cdot p^{m-\nu} \cdot p^{(\nu-m)s}$$

$$= \sum_{\nu=0}^{2m}{}' \sigma_{2m-\nu} p^{-\frac{m}{2}} \cdot p^{\nu-m} \cdot p^{(m-\nu)s}.$$

Vergleicht man gleiche Potenzen von p^s, so resultiert

$$\sigma_\nu p^{-\frac{m}{2}} = \sigma_{2m-\nu} p^{-\frac{m}{2}} p^{\nu-m}.$$

Daraus ergibt sich sofort unsere Reziprozitätsbeziehung:

$$\sigma_{2m-\nu} = p^{m-\nu}\sigma_\nu; \tag{10}$$

speziell für $\nu = 0$ wegen $\sigma_0 = 1$,

$$\sigma_{2m} = p^m. \tag{11}$$

Aus § 18, (10) folgt also

$$h = (1+p^m) + (1+p^{m-1})\sigma_1 + (1+p^{m-2})\sigma_2 + \ldots + (1+p)\sigma_{m-1} + \sigma_m. \tag{12}$$

Dies erleichtert sehr die Berechnung der Klassenzahl, da die Berechnung von σ_ν für höhere Werte von ν recht mühselig ist.

2. Grad von D gerade: $|D| = p^{2m}$. Körper imaginär. Hier ist nach (4)

$$\begin{aligned} \Xi(s) &= (1-p^{-2(s-1)})(\sqrt{|D|})^{s-\frac{1}{2}} Z(s) \\ &= (1+p^{-(s-1)})\, p^{m(s-\frac{1}{2})} \cdot \sum_{\nu=0}^{2m-1} \frac{\sigma_\nu}{p^{\nu s}} \\ &= p^{-\frac{m}{2}} \left(1+\frac{p}{p^s}\right) \cdot \sum_{\nu=0}^{2m-1} \sigma_\nu p^{(m-\nu)s} \\ &= p^{-\frac{m}{2}} \left(\sum_{\nu=0}^{2m-1} \sigma_\nu p^{(m-\nu)s} + \sum_{\nu=0}^{2m-1} p\,\sigma_\nu p^{(m-\nu-1)s} \right) \\ &= p^{-\frac{m}{2}} \left(p^{ms} + \frac{p\sigma_{2m-1}}{p^{ms}} + \sum_{\nu=1}^{2m-1} (\sigma_\nu + p\sigma_{\nu-1}) p^{(m-\nu)s} \right) \end{aligned} \tag{13}$$

eine Funktion mit der Funktionalgleichung (9). Wegen

$$\begin{aligned} \Xi(1-s) &= p^{-\frac{m}{2}} \left(\frac{p^m}{p^{ms}} + \frac{\sigma_{2m-1}}{p^{m-1}} p^{ms} + \sum_{\nu=1}^{2m-1} (\sigma_\nu + p\sigma_{\nu-1}) p^{m-\nu} p^{(\nu-m)s} \right) \\ &= p^{-\frac{m}{2}} \left(\frac{p^m}{p^{ms}} + \frac{\sigma_{2m-1}}{p^{m-1}} p^{ms} + \sum_{\nu=1}^{2m-1} (\sigma_{2m-\nu} + p\sigma_{2m-\nu-1}) p^{\nu-m} p^{(m-\nu)s} \right) \end{aligned}$$

erhält man hier

$$\sigma_{2m-\nu} + p\sigma_{2m-\nu-1} = p^{m-\nu}(\sigma_\nu + p\sigma_{\nu-1}), \qquad 1 \leqq \nu \leqq 2m-1; \tag{14}$$

und

$$\sigma_{2m-1} = p^{m-1}. \tag{15}$$

Durch einfache Rechnung erhält man daraus

$$\sigma_{2m-\nu} = p^{m-\nu}[\sigma_{\nu-1} + (p-1)(\sigma_{\nu-2} - \sigma_{\nu-3} + \sigma_{\nu-4} - + \ldots + (-1)^{\nu-2}\sigma_0)], \tag{16}$$

gültig für $2 \leqq \nu \leqq 2m$.

Die Beziehungen (15) und (16) ergeben nun aus $\sigma_0, \sigma_1, \sigma_2, \ldots, \sigma_{m-1}$ die m übrigen Größen, indem (16) für $2 \leqq \nu \leqq m$ verwendet wird. Aus

$$h = \sum_{\nu=0}^{2m-1} \sigma_\nu$$

berechnet sich dann die Klassenzahl. Wir wollen den Ausdruck, der nichts Bemerkenswertes bietet, nicht erst hinschreiben.

Mit Hilfe von § 17, (6) finden wir aus (14), (15), (16) sofort die entsprechenden Formeln für reelle Körper:

$$(17) \quad \sigma_{2m-\nu} - p\sigma_{2m-\nu-1} = p^{m-\nu}(\sigma_\nu - p\sigma_{\nu-1}), \qquad 1 \leqq \nu \leqq 2m-1;$$

$$(18) \quad \sigma_{2m-1} = -p^{m-1};$$

$$(19) \quad \sigma_{2m-\nu} = p^{m-\nu}[-\sigma_{\nu-1} + (p-1)(\sigma_{\nu-2} + \sigma_{\nu-3} + \sigma_{\nu-4} + \ldots + \sigma_1 + \sigma_0)],$$

gültig für $2 \leqq \nu \leqq 2m$.

Aus ihnen und

$$h = -\frac{1}{R} \sum_{\nu=1}^{2m-1} \nu\sigma_\nu$$

ergibt sich die Klassenzahl.

§ 22.

Die Anzahl der Ideale und Primideale gegebener Absolutnorm.

Es ist

$$Z(s) = \frac{1}{1-p^{-(s-1)}} \cdot \sum_{\nu=0}^{n-1} \frac{\sigma_\nu}{p^{\nu s}} = \sum_{\mu=0}^{\infty} \frac{p^\mu}{p^{\mu s}} \cdot \sum_{\nu=0}^{n-1} \frac{\sigma_\nu}{p^{\nu s}}.$$

Daraus folgt

$$Z(s) = 1 + \frac{p\sigma_0 + \sigma_1}{p^s} + \frac{p^2\sigma_0 + p\sigma_1 + \sigma_2}{p^{2s}} + \ldots + \frac{p^{n-2}\sigma_0 + p^{n-3}\sigma_1 + \ldots + \sigma_{n-2}}{p^{(n-2)s}} + \sum_{\nu=n-1}^{\infty} \frac{p^\nu\sigma_0 + p^{\nu-1}\sigma_1 + \ldots + p^{\nu-(n-1)}\sigma_{n-1}}{p^{\nu s}}.$$

Bezeichnet man nun mit $H(x)$ die Anzahl der Ideale mit $|N\mathfrak{a}| = x$, so ist andererseits

$$Z(s) = \sum_{\mathfrak{a}} \frac{1}{|N\mathfrak{a}|^s} = \sum_{\nu=0}^{\infty} \frac{H(p^\nu)}{p^{\nu s}}.$$

Es ist also für $\nu \geqq n-1$

$$H(p^\nu) = p^\nu\sigma_0 + p^{\nu-1}\sigma_1 + \ldots + p^{\nu-(n-1)}\sigma_{n-1} = p^\nu \sum_{\mu=0}^{n-1} \frac{\sigma_\mu}{p^\mu} = \frac{h}{\varkappa} p^\nu,$$

wo $\varkappa$ durch § 20, (1) gegeben ist. $H(x)$ hat natürlich nur einen Sinn,

wenn x von der Form p^r ist, und dies wollen wir voraussetzen. Dann ist aber

$$H(x) = \frac{h}{x} x \quad \text{für} \quad x \geqq \frac{|D|}{p}. \tag{1}$$

Für $x < \frac{|D|}{p}$ ist der Ausdruck anders, doch kommt dies für unsere asymptotischen Überlegungen nicht in Betracht. Aus

$$Z(s) = \frac{1}{1-p^{-(s-1)}}\left(\sigma_0 + \frac{\sigma_1}{p^s} + \frac{\sigma_2}{p^{2s}} + \ldots + \frac{\sigma_{n-1}}{p^{(n-1)s}}\right)$$

erkennen wir, daß alle Nullstellen ϱ von $Z(s)$ durch den zweiten Term geliefert werden. Setzt man $p^s = z$, so erhält man zur Bestimmung der Nullstellen die algebraische Gleichung

$$z^{n-1} + \sigma_1 z^{n-2} + \sigma_2 z^{n-3} + \ldots + \sigma_{n-1} = 0. \tag{2}$$

Nennen wir ihre Wurzeln $\beta_1, \beta_2, \ldots, \beta_{n-1}$ (diese Bezeichnung werde auch weiterhin festgehalten), so finden wir die Nullstellen ϱ der Zetafunktion durch die Gleichung

$$\beta_\nu = p^\varrho. \tag{3}$$

Dadurch werden aber auch die trivialen Nullstellen auf $\Re(s) = 0$ gegeben.

Wenn also der Grad von D gerade ist, hat (2) die einfache Wurzel $+1$ oder -1, je nachdem der Körper reell oder imaginär ist. Wenn D ungeraden Grad hat, gibt es keine „triviale" Wurzel von (2).

Ist $D = at + b$ linear, so ist (2) von nulltem Grade, $Z(s)$ hat also überhaupt keine Wurzeln.

Ist D quadratisch, so ist (2) vom ersten Grade, $Z(s)$ hat also nur triviale Wurzeln.

Nicht triviale Wurzeln sind also erst von kubischem D an vorhanden.

Sei nun θ die obere Grenze der reellen Teile der Nullstellen von $Z(s)$. Von den beiden besprochenen Ausnahmefällen, wo überhaupt keine Wurzel vorhanden oder $\theta = 0$ ist, abgesehen, ist dann stets

$$\frac{1}{2} \leqq \theta < 1.$$

Aus (3) folgt dann

$$\beta_\nu \leqq p^\theta \qquad (\tfrac{1}{2} \leqq \theta < 1), \tag{4}$$

und (4) ist jedenfalls auch in den Ausnahmefällen richtig. θ hängt dabei nur vom Körper ab.

Für $Z(s)$ erhält man nun die Produktdarstellung

$$Z(s) = \frac{1}{1-p^{-(s-1)}} \cdot \prod_{\nu=1}^{n-1} (1 - \beta_\nu p^{-s}). \tag{5}$$

Einerseits ist also

$$\log Z(s) = -\log(1-p^{-(s-1)}) + \sum_{u=1}^{n-1} \log(1-\beta_u p^{-s})$$

$$= -\sum_{\nu=1}^{\infty}{}' \frac{p^\nu - \beta_1^\nu - \beta_2^\nu - \ldots - \beta_{n-1}^\nu}{\nu \cdot p^{\nu s}} \quad \text{für} \quad \Re(s) > 1. \tag{6}$$

Andererseits aber ist, wenn $\pi(x)$ die Anzahl der Primideale $\mathfrak{p}$ mit der Absolutnorm $|N\mathfrak{p}| = x$ bedeutet (wo x wieder nur die Werte p^ν annehmen soll):

$$\log Z(s) = -\sum_{\mathfrak{p}}{}' \log(1-|N\mathfrak{p}|^{-s}) = \sum_{\mathfrak{p},\,\nu \geqq 1}{}' \frac{1}{\nu\,|N\mathfrak{p}^\nu|^s}$$

$$= \sum_{\nu=1}^{\infty}{}' \frac{\sum_{d|\nu}{}' \frac{\pi(p^d)}{\frac{\nu}{d}}}{p^{\nu s}} = \sum_{\nu=1}^{\infty}{}' \frac{\sum_{d|\nu}{}' d\,\pi(p^d)}{\nu\, p^{\nu s}} \quad \text{für} \quad \Re(s) > 1. \tag{7}$$

Aus (6) und (7) folgt aber

$$\sum_{d|\nu}{}' d\,\pi(p^d) = p^\nu - \beta_1^\nu - \beta_2^\nu - \ldots - \beta_{n-1}^\nu. \tag{8}$$

Es ist dies die genaue Formel für $\pi(x)$ und etwa die Analogie zu der Riemann-Mangoldtschen Formel.

Nach unseren Resultaten über die Norm von Primidealen ist nun $\pi(p^d)$ höchstens gleich der doppelten Anzahl der Primfunktionen des Grades d plus der Anzahl der Primfunktionen vom Grade $\frac{d}{2}$. Es gibt also eine absolute Konstante C, so daß

$$\pi(p^d) \leqq C \cdot \frac{p^d}{d}.$$

Spaltet man also in (8) den Teiler $d = \nu$ ab, so ist der Rest sicher kleiner als

$$\tfrac{\nu}{2}\,\pi(p^{\frac{\nu}{2}}) + \tfrac{\nu}{3}\,\pi(p^{\frac{\nu}{3}}) + \ldots + \tfrac{\nu}{\nu}\,\pi(p^{\frac{\nu}{\nu}})$$

$$\leqq C(p^{\frac{\nu}{2}} + p^{\frac{\nu}{3}} + p^{\frac{\nu}{4}} + \ldots + p^{\frac{\nu}{\nu}})$$

$$\leqq C(p^{\frac{\nu}{2}} + \nu p^{\frac{\nu}{3}}) = O(p^{\frac{\nu}{2}}).$$

Also wird

$$\nu \cdot \pi(p^\nu) + O(p^{\frac{\nu}{2}}) = p^\nu - \beta_1^\nu - \beta_2^\nu - \ldots - \beta_{n-1}^\nu.$$

Wegen (4) ist

$$|\beta_\varkappa^\nu| \leqq p^{\vartheta\nu};$$

also ist:

$$\nu \cdot \pi(p^\nu) = p^\nu + O(p^{\frac{\nu}{2}}) + O(p^{\theta\nu}) = p^\nu + O(p^{\theta\nu}),$$

$$\pi(p^\nu) = \frac{p^\nu}{\nu} + O\left(\frac{p^{\theta\nu}}{\nu}\right).$$

Da nun, wenn $x = p^\nu$ gesetzt wird, $\nu = \frac{\log x}{\log p}$ ist, erhalten wir:

$$\pi(p^\nu) = \frac{x}{\log x} \cdot \log p + O\left(\frac{x^\theta}{\log x}\right), \tag{9}$$

wo $\frac{1}{2} \leqq \theta < 1$.

§ 23.

Tafeln der Klassenzahl.

Im folgenden soll eine kleine Tafel für die Klassenzahlen wiedergegeben werden. Zunächst wollen wir aber die bereits gefundenen Resultate für quadratisches D bestätigen.

1. $\sqrt{D}$ imaginär; $|D| = p^2$; $m = 1$; $h = \sigma_0 + \sigma_1 = 1 + \sigma_1$. Nach § 21, (15) ist $\sigma_1 = 1$, also $h = 2$.

2. $\sqrt{D}$ reell. Nach § 21, (18) ist $\sigma_1 = -1$, so daß § 21, (7) ergibt $h = \frac{1}{R}$. Also muß $R = 1$; $h = 1$ sein.

Für kubische Diskriminanten ist $m = 1$ und § 21, (12) ergibt

$$h = p + 1 + \sigma_1. \tag{1}$$

Bei der Herstellung einer Tafel beachte man weiter, daß t einer geeigneten linearen Transformation $t' = at + b$ unterworfen werden kann, ohne die Klassenzahl zu ändern. Da ferner $\sigma_1(gD) = -\sigma_1(D)$ ist, findet man aus (1)

$$h_D + h_{gD} = 2(p + 1). \tag{2}$$

Aus der Klassenzahl von $K(\sqrt{D})$ findet man also, wenn D kubisch ist, ohne weiteres die Klassenzahl von $K(\sqrt{gD})$.

Durch lineare Transformation von t können wir uns (nachdem ein eventueller quadratischer Rest abgestoßen ist) D in die Form gesetzt denken:

$$D = t^3 + at + b.$$

Nur im Falle $p = 3$ geht dies nicht. Die Berechnung von σ_1 ist nun sehr einfach:

$$\sigma_1 = \sum_{c=1}^{p-1} \left[\frac{t^3 + at + b}{t - c}\right]$$

(wobei eventuelle Linearteiler von D wegzulassen sind). Nun ist

$$\left[\frac{t^3 + at + b}{t - c}\right] = \left[\frac{c^3 + ac + b}{t - c}\right] = \left(\frac{c^3 + ac + b}{p}\right),$$

also

$$\sigma_1 = \sum_{c=0}^{p-1} \left(\frac{c^3 + ac + b}{p} \right).$$

Es ist also σ_1 in einfachster Weise durch Legendresymbole ausgedrückt.

Beispiel. $p = 7$, $D = t^3 + 3t + 2$ (Primfunktion).

$$\sigma_1 = \left(\frac{2}{7}\right) + \left(\frac{6}{7}\right) + \left(\frac{2}{7}\right) + \left(\frac{3}{7}\right) + \left(\frac{1}{7}\right) + \left(\frac{2}{7}\right) + \left(\frac{5}{7}\right)$$
$$= 1 - 1 + 1 - 1 + 1 + 1 - 1 = 1.$$

Somit $h = 9$. Dies ist auch die Klassenzahl für die durch Lineartransformation hervorgehenden Diskriminanten $t^3 - 3t + 2$, $t^3 - t + 2$. Dagegen haben die Diskriminanten gD, das sind (nach Lineartransformation) $t^3 + 3t - 2$, $t^3 - 2t - 2$, $t^3 - t - 2$, die Klassenzahl $h = 7$ (nach (2)).

Auf diese Art wurde Tabelle I berechnet, welche die Klassenzahlen für $p = 3$, $p = 5$, $p = 7$ gibt.

Die zugehörige Gleichung für die Nullstellen von $Z(s)$ lautet

$$z^2 + \sigma_1 z + p = 0.$$

Ihre Wurzeln sind

$$\beta = -\frac{\sigma_1}{2} \pm \frac{1}{2}\sqrt{\sigma_1^2 - 4p}.$$

Sind sie komplex, so ist $\beta_1 = \sqrt{p}$, also wenn ϱ die Nullstellen von $Z(s)$ sind, $\Re(\varrho) = \frac{1}{2}$. Dies erfordert

$$-2\sqrt{p} < \sigma_1 < 2\sqrt{p},$$

oder

für $p = 3$: $\quad -3 \leqq \sigma_1 \leqq +3$,
für $p = 5$: $\quad -4 \leqq \sigma_2 \leqq +4$,
für $p = 7$: $\quad -5 \leqq \sigma_1 \leqq +5$.

Die Tabelle lehrt, daß diese Relationen wirklich erfüllt sind.

Also liegen die Nullstellen alle auf $\Re(s) = \frac{1}{2}$.

Für biquadratische D ergibt sich im imaginären Falle: $\sigma_3 = p$, $\sigma_2 = p - 1 + \sigma_1$. Also ist

$$h = 2p + 2\sigma_1.$$

Auch hier genügt die Berechnung von σ_1. Für $p = 3$ ist $g = -1$. Dies liefert Tabelle II.

Für reelle Körper ist $\sigma_3 = -p$, $\sigma_2 = p - 1 - \sigma_1$, also

$$h = -\frac{1}{R}(\sigma_1 + 2\sigma_2 + 3\sigma_3) = \frac{1}{R}(p + 2 + \sigma_1).$$

I.

$p=3$

D	Zerlegung	σ_1	h	D	Zerlegung	σ_1	h
t^3+t^2+t+1	$(t+1)(t^2+1)$			t^3-t^2+t+1			
t^3+t^2+1	$(t-1)(t^2-t-1)$	$+2$	6	t^3-t^2+1		$+1$	5
t^3+t^2-t	$t(t^2+t-1)$			t^3-t^2-t-1	Primfunktion		
t^3-t^2+t-1	$(t-1)(t^2+1)$			t^3-t+1		$+3$	7
t^3-t^2-1	$(t+1)(t^2+t-1)$	-2	2	t^3-t-1		-3	1
t^3-t^2-t	$t(t^2-t-1)$			t^3+t+1	$(t-1)(t^2+t-1)$		
t^3+t^2+t-1				t^3+t-1	$(t+1)(t^2-t-1)$	0	4
t^3+t^2-1	Primfunktion	-1	3	t^3+t	$t(t^2+1)$		
t^3+t^2-t+1				t^3-t	$t(t-1)(t+1)$		

$p=5$

D	Zerlegung	σ_1	h	D	Zerlegung	σ_1	h
t^3+1	$(t+1)(t^2-t+1)$			t^3+2t	$t(t^2+2)$	-4	2
t^3-1	$(t-1)(t^2+t+1)$	0	6	t^3-2t	$t(t^2-2)$	$+4$	10
t^3+2	$(t-2)(t^2+2t-1)$			t^3+t+1		$+3$	9
t^3-2	$(t+2)(t^2-2t-1)$			t^3+t-1			
t^3-t+1	$(t+2)(t^2-2t-2)$			t^3-t+2		-3	3
t^3-t-1	$(t-2)(t^2+2t-2)$	$+2$	8	t^3-t-2	Primfunktion		
t^3-t	$t(t-1)(t+1)$			t^3+2t+1		$+1$	7
t^3+t+2	$(t+1)(t^2-t+2)$			t^3+2t-1			
t^3+t-2	$(t-1)(t^2+t+2)$	-2	4	t^3-2t+2		-1	5
t^3+t	$t(t+2)(t-2)$			t^3-2t-2			

$p=7$

D	Zerlegung	σ_1	h	D	Zerlegung	σ_1	h
t^3+1	$(t+1)(t-3)(t+2)$			t^3-1	$(t-1)(t+3)(t-2)$		
t^3-t+1	$(t-2)(t^2+2t+3)$	$+4$	12	t^3-t-1	$(t+2)(t^2-2t+3)$	-4	4
t^3-2t+1	$(t-1)(t^2+t-1)$			t^3-2t-1	$(t+1)(t^2-t-1)$		
t^3+3t+1	$(t+3)(t^2-3t-2)$			t^3+3t-1	$(t-3)(t^2+3t-2)$		
t^3+t+3	$(t+2)(t^2-2t-2)$			t^3+t-3	$(t-2)(t^2+2t-2)$		
t^3+2t+3	$(t+1)(t^2-t+3)$			t^3+2t-3	$(t-1)(t^2+t+3)$		
t^3-3t+3	$(t-3)(t^2+3t-1)$			t^3-3t-3	$(t+3)(t^2-3t-1)$		
t^3-t+3	$(t+3)(t^2-3t+1)$	-2	6	t^3-t-3	$(t-3)(t^2+3t+1)$	$+2$	10
t^3-2t+3	$(t-2)(t^2+2t+2)$			t^3-2t-3	$(t+2)(t^2-2t+2)$		
t^3+3t+3	$(t-1)(t^2+t-3)$			t^3+3t-3	$(t+1)(t^2-t-3)$		
t^3+t	$t(t^2+1)$			t^3-t	$t(t+1)(t-1)$		
t^3+2t	$t(t^2+2)$	0	8	t^3-2t	$t(t+3)(t-3)$	0	8
t^3-3t	$t(t^2-3)$			t^3+3t	$t(t+2)(t-2)$		

$p = 7$. Primfunktionen

D	σ_1	h	D	σ_1	h	D	σ_1	h	D	σ_1	h
t^3-t-2			t^3+3	$+5$	13	t^3-3	-5	3	t^3-t+2		
t^3-2t-2	-1	7	t^3+t+1			t^3+t-1			t^3-2t+2	$+1$	9
t^3+3t-2			t^3+2t+1	-3	5	t^3+2t-1	$+3$	11	t^3+3t+2		
t^3-2			t^3-3t+1			t^3-3t-1			t^3+2		

II.

$p = 3$

D	Zerlegung	σ_1	h	D	Zerlegung	σ_1	h
$-(t^4+1)$	$-(t^2+t-1)(t^2-t-1)$			$-(t^4+t^2+t-1)$	$-(t+1)(t^3-t^2-t-1)$	$+2$	10
$-(t^4-1)$	$-(t-1)(t+1)(t^2+1)$	$+1$	8	$-(t^4+t^2-t-1)$	$-(t-1)(t^3+t^2-t+1)$		
(t^4+t-1)				$-(t^4+t+1)$	$-(t-1)(t^3+t^2+t-1)$	-2	2
(t^4-t-1)				$-(t^4-t+1)$	$-(t+1)(t^3-t^2+t+1)$		
(t^4+t^2-1)	Primfunktion			$-(t^4-t^2+t)$	$-t(t^3-t+1)$		
(t^4+t^2+t+1)				$-(t^4-t^2-t)$	$-t(t^3-t-1)$	0	6
(t^4+t^2-t+1)		-1	4	$-(t^4-t^2+t+1)$	$-(t+1)(t^3-t^2+1)$		
(t^4+t^2+t)	$-t(t-1)(t^2+t-1)$			$-(t^4-t^2-t+1)$	$-(t-1)(t^3+t^2-1)$		
(t^4+t^2-t)	$-t(t+1)(t^2-t-1)$			$-(t^4-t^2-1)$	Primfunktion	$+3$	12

III.

$p = 3$ reelle Körper.

D	ε_0	R	σ_1	h
t^4+t+1	$(t^7-t^6-t^5+t^4+t^3-t^2+1)+(t^5-t^4-t^3-t^2+t)\sqrt{D}$	7	$+2$	
t^4-t+1	$(t^7+t^6-t^5-t^4+t^3+t^2-1)+(t^5+t^4-t^3+t^2+t)\sqrt{D}$	7	$+2$	
t^4+t^2+t+1	$(t^6-t^5-t^4+t^3-t^2+t)+(t^4-t^3+t+1)\sqrt{D}$	6	$+1$	
t^4+t^2-t+1	$(t^6+t^5-t^4-t^3-t^2-t)+(t^4+t^3-t+1)\sqrt{D}$	6	$+1$	
t^4-t^2+t	$(t^5-t^4-t^2+t-1)+(t^3-t^2-t+1)\sqrt{D}$	5	0	
t^4-t^2-t	$(t^5+t^4+t^2+t+1)+(t^3+t^2-t-1)\sqrt{D}$	5	0	
t^4-t^2+t+1	$(t^5-t^4+t^2-1)+(t^3-t^2-t)\sqrt{D}$	5	0	1
t^4-t^2-t+1	$(t^5+t^4-t^2+1)+(t^3+t^2-t)\sqrt{D}$	5	0	
t^4+t-1	$(t^4-t^3-t^2-t-1)+(t^2-t-1)\sqrt{D}$	4	-1	
t^4-t-1	$(t^4+t^3-t^2+t-1)+(t^2+t-1)\sqrt{D}$	4	-1	
t^4+t^2+t-1	$(t^3-t^2-t)+(t-1)\sqrt{D}$	3	-2	
t^4+t^2-t-1	$(t^3+t^2-t)+(t+1)\sqrt{D}$	3	-2	
t^4-t^2-1	$(t^2+1)+\sqrt{D}$	2	-3	
t^4+t^2+t	$(t^3+t^2-t+1)+(t+1)\sqrt{D}$	3	$+1$	
t^4+t^2-t	$(t^3-t^2-t-1)+(t-1)\sqrt{D}$	3	$+1$	2
t^4+1	$t^2+\sqrt{D}$	2	-1	
t^4-1	$t^2+\sqrt{D}$	2	-1	
t^4+t^2-1	$(t^2-1)+\sqrt{D}$	2	$+1$	3

Sei nun σ_1' die σ-Summe des imaginären Körpers $K(\sqrt{D})$. Dann ist $\sigma_1' = -\sigma_1$. Also

$$h = \frac{1}{R}(p + 2 - \sigma_1').$$

Aus der Tabelle II lesen wir für die verschiedenen Gruppen die Klassenzahlen $\frac{4}{R}, \frac{6}{R}, \frac{3}{R}, \frac{7}{R}, \frac{5}{R}, \frac{2}{R}$ ab. Da sowohl h wie R ganzzahlig und wegen $|\varepsilon_0| \geqq \sqrt{D} = p^2$, $R \geqq 2$ ist, ergeben sich für die vier letzten Fälle: $R = 3, 7, 5, 2$, also $h = 1$. Eine einfache Diskussion liefert auch die Entscheidung in den übrigen Fällen.

In Tabelle III ist dies im Falle $p = 3$ zusammengestellt. Wir geben auch die expliziten Werte der Grundeinheiten, aus denen wir die Richtigkeit der vorigen Diskussion bestätigen.

Was nun die Nullstellen von $Z(s)$ anbetrifft, so haben wir die Gleichung

$$z^3 + \sigma_1 z^2 + \sigma_2 z + p$$

(wobei es genügt, den imaginären Fall zu betrachten). Nach Abspaltung des trivialen Faktors $z + 1$ unter Berücksichtigung der Relation $\sigma_2 = p - 1 + \sigma_1$ erhält man

$$z^2 + (\sigma_1 - 1)z + p = 0.$$

Sind die Wurzeln komplex, so liegen wieder die Nullstellen auf $\Re(\varrho) = \frac{1}{2}$. Dies ist dann und nur dann der Fall, wenn

$$-2\sqrt{p} < \sigma_1 - 1 < 2\sqrt{p},$$

also für $p = 3$:

$$-2 \leqq \sigma_1 \leqq 4.$$

Dies ist aber der Fall.

Für $p = 5$ müßte $-3 \leqq \sigma_1 \leqq 5$ sein. Wir zeigen noch, daß dies zutrifft. Trivial ist zunächst $-5 \leqq \sigma_1 \leqq 5$. Nun ist aber $\sigma_1 = -5$ unmöglich, da sonst $h = 0$ wäre. Es ist also noch $\sigma_1 = -4$ in Betracht zu ziehen. Dann muß σ_1 die Summe von genau vier Symbolen $\left[\frac{D}{t-c}\right]$ sein (da bei fünf Symbolen σ_1 ungerade ist), deren jedes den Wert -1 hat. D muß also einen und nur einen Linearfaktor enthalten, den wir nach passender Lineartransformation als t selbst nehmen können. Also, da $g = 2$ ist: $D = 2tD_1$ ($\operatorname{sgn} D_1 = 1$, D_1 Primfunktion). Nun ist

$$\left[\frac{D}{t-1}\right] = \left[\frac{D_1}{t-1}\right], \quad \left[\frac{D}{t-2}\right] = \left[\frac{D_1}{t-2}\right], \quad \left[\frac{D}{t-3}\right] = \left[\frac{D_1}{t-3}\right], \quad \left[\frac{D}{t-4}\right] = -\left[\frac{D_1}{t-4}\right].$$

Also ist

$$\left[\frac{D_1}{t-1}\right] = 1, \quad \left[\frac{D_1}{t-2}\right] = -1, \quad \left[\frac{D_1}{t-3}\right] = -1, \quad \left[\frac{D_1}{t-4}\right] = 1.$$

Nennen wir σ_1' die σ-Summe in $K(\sqrt{D_1})$, so ist, da D_1 Primfunktion ist, nach dem eben Gezeigten $\sigma_1 = \left[\frac{D_1}{t}\right] = \pm 1$. Nach Tabelle I hat also D_1 die Form $(t+a)^3 + 2(t+a) + 1$ oder $(t+a)^3 - 2(t+a) + 2$. Eine Durchrechnung der fünf sich schließlich ergebenden Fälle ergibt $\sigma_1 \neq -4$, so daß wieder $\Re(\varrho) = \frac{1}{2}$ ist.

Endlich wurde im Falle $p = 3$ durch ähnliche Diskussion gezeigt, daß auch im Falle $n = 5$ alle Nullstellen auf der Geraden $\Re(\varrho) = \frac{1}{2}$ liegen. Der Diskussion entziehen sich nur die Primfunktionen, für die also die Rechnung darüber zu entscheiden hat.

§ 24.

Der Zusammenhang zwischen der Klassenzahl und den Nullstellen von $Z(s)$. — Die Anzahl der Klassen in den Geschlechtern imaginärer Körper.

Wir kehren nun zur Formel § 22, (5) zurück:

$$Z(s) = \frac{1}{1-p^{-(s-1)}} \cdot \prod_{\nu=1}^{n-1} (1 - \beta_\nu p^{-s}). \tag{1}$$

Nach § 18 gilt nun für imaginäre Körper ($n \geqq 2$):

$$h = -wZ(0) = \prod_{\nu=1}^{n-1} (1 - \beta_\nu), \tag{2}$$

wo β_ν die Wurzeln von $z^{n-1} + \sigma_1 z^{n-2} + \ldots + \sigma_{n-1} = 0$ sind, und $\beta_\nu = p^\varrho$, wo ϱ die Nullstellen von $Z(s)$ durchläuft.

In (1) möge β_{n-1} die triviale Wurzel sein (falls eine vorkommt).

Für reelle Körper ist $\beta_{n-1} = -1$, und aus § 21 folgt

$$h = -\frac{p-1}{R \log p} \lim_{s=0} \frac{Z(s)}{s} = \frac{1}{R} \prod_{\nu=1}^{n-2} (1 - \beta_\nu).$$

Demnach haben wir, wenn β_ν nur die nicht trivialen Wurzeln bedeutet:

$$h = \prod_{\nu=1}^{n-1} (\beta_\nu - 1), \quad \text{falls } n \text{ ungerade}, \tag{3}$$

$$h = 2 \cdot \prod_{\nu=1}^{n-1} (\beta_\nu - 1), \quad \text{falls } n \text{ gerade, Körper imaginär}, \tag{4}$$

$$h = \frac{1}{R} \cdot \prod_{\nu=1}^{n-2} (\beta_\nu - 1), \quad \text{falls } n \text{ gerade, Körper reell}. \tag{5}$$

Ist nun β_ν die Wurzel in $K(\sqrt{D})$, so ist $-\beta_\nu$ wegen $\sigma_\nu(D) = (-1)^\nu \sigma_\nu(gD)$ die Wurzel in $K(\sqrt{D})$. Nennt man also h' die Klassenzahl im letzteren Körper, so erhält man aus (3), (4), (5):

$$(6) \qquad h h' = \prod_{\nu=1}^{n-1} (\beta_\nu^2 - 1), \quad \text{falls } n \text{ ungerade.}$$

$$(7) \qquad h h' = \frac{2}{R} \prod_{\nu=1}^{n-2} (\beta_\nu^2 - 1), \quad \text{falls } n \text{ gerade.}$$

Nun brauchen wir noch eine einfache Abschätzung von h. Es ist, der Bedeutung von σ_ν nach, $|\sigma_\nu| \leqq p^\nu$.

1. n ungerade. $\sigma_{2m-\nu} = p^{m-\nu} \cdot \sigma_\nu$. Also $|\sigma_{2m-\nu}| \leqq p^m$, somit $|\sigma_\nu| \leqq p^m$. Wegen

$$h = \prod_{\nu=0}^{n-1} \sigma_\nu$$

ist also

$$(8) \qquad h \leqq n \cdot p^m = n(\sqrt{p})^{n-1}.$$

2. n gerade, Körper reell. Aus § 21, (19) folgt

$$|\sigma_{2m-\nu}| \leqq p^{m-\nu}(p^{\nu-1} + (p-1)(p^{\nu-2} + p^{\nu-3} + \ldots + p + 1)$$
$$= p^{m-\nu}(2p^{\nu-1} - 1) < 2p^{m-1}.$$

Aus § 21 (7) also

$$(9) \qquad h \leqq \frac{2}{R} \cdot (n-1)^2 p^{m-1} = \frac{2}{R}(n-1)^2 (\sqrt{p})^{n-2}.$$

Es werde nun die Richtigkeit der Riemannschen Vermutung vorausgesetzt. Dann ist $|\beta_\nu| = \sqrt{p}$. Es sei nun $K(\sqrt{D})$ ein imaginärer Körper. Die Fälle $n = 1$, $n = 2$ lassen wir als genau bekannt beiseite. Es sei also $n \geqq 3$. Dann folgt aus (3) und (4)

$$(10) \qquad (\sqrt{p} - 1)^{n-1} \leqq h \leqq (\sqrt{p} + 1)^{n-1}, \quad \text{falls } n \text{ ungerade,}$$

$$(11) \qquad 2(\sqrt{p} - 1)^{n-2} \leqq h \leqq 2(\sqrt{p} + 1)^{n-2}, \quad \text{falls } n \text{ gerade,}$$

Die unteren Grenzen sind aber für $p = 3$ trivial. Deshalb haben wir noch andere Formeln abzuleiten. Aus (6) und (7) folgt nämlich

$$(12) \qquad h h' \geqq (p-1)^{n-1}, \quad \text{falls } n \text{ ungerade,}$$

$$(13) \qquad h h' \geqq \frac{2}{R}(p-1)^{n-2}, \quad \text{falls } n \text{ gerade.}$$

Wenden wir nun auf h' die Formeln (8) und (9) an, so resultiert

$$(14) \qquad h \geqq \frac{1}{n}\left(\frac{p-1}{\sqrt{p}}\right)^{n-1}, \quad \text{falls } n \text{ ungerade,}$$

$$(15) \qquad h \geqq \frac{1}{(n-1)^2}\left(\frac{p-1}{\sqrt{p}}\right)^{n-2}, \quad \text{falls } n \text{ gerade.}$$

Für $p = 3$ folgt daraus

$$h > \frac{1}{n}(1{,}15)^{n-1} \quad \text{bzw.} \quad h \geqq \frac{1}{(n-1)^2}(1{,}15)^{n-2}.$$

Daraus und aus (10) und (11) folgt nun, daß es nur endlich viele Körper gegebener Klassenzahl gibt, sogar wenn p und $n \geqq 3$ gleichzeitig variieren. Aus (10) und (11) folgt insbesondere, daß es für $p \geqq 5$, $n \geqq 3$ keine Körper mit der Klassenzahl 1 gibt. Für $p = 3$ gibt es noch endlich viele. Wahrscheinlich ist aber $K(\sqrt{t^3 - t - 1})$ der einzige Körper mit der Klassenzahl 1.

Nennen wir nun f die Anzahl der Klassen eines Geschlechtes und s die Anzahl der Primfaktoren von D, so ist nach § 11

$$f \geqq \frac{h}{2^{s-1}}.$$

Also haben wir

$$f \geqq \frac{(\sqrt{p}-1)^{n-1}}{2^{s-1}} \quad (n \text{ ungerade}),$$

$$f \geqq \frac{(\sqrt{p}-1)^{n-2}}{2^{s-2}} \quad (n \text{ gerade}).$$

Nun ist sicher $s \leqq n$. Es ist nämlich nur dann $s = n$, wenn alle Primfaktoren linear sind. Also haben wir

$$f \geqq \left(\frac{\sqrt{p}-1}{2}\right)^{n-1} \quad (n \text{ ungerade}),$$

$$f \geqq \left(\frac{\sqrt{p}-1}{2}\right)^{n-2} \quad (n \text{ gerade}).$$

Dies ergibt für $p \geqq 11$, $n \geqq 3$ stets $f > 1$, so daß es also für $p \geqq 11$, $n \geqq 3$ keine Körper mit einklassigen Geschlechtern gibt. Es zeigt sich sogar, daß dann f mit n und p (jedes auch einzeln) über alle Grenzen wächst, so daß es nur endlich viele Körper gibt mit vorgeschriebener Anzahl von Klassen in jedem Geschlecht. Dies haben wir noch für $p = 7, 5, 3$ zu zeigen.

Für $p = 7$ folgt aus (14), (15)

$$f \geqq \frac{1}{n}\left(\frac{6}{2\sqrt{7}}\right)^{n-1} \quad (n \text{ ungerade}),$$

$$f \geqq \frac{1}{2(n-1)^2}\left(\frac{6}{2\sqrt{7}}\right)^{n-2} \quad (n \text{ gerade}).$$

Dies liefert unmittelbar das Gewünschte.

Für $p = 5$ liefert (14), (15):

$$h \geqq \frac{1}{n}(1{,}78)^{n-1} \quad \text{bzw.} \quad h \geqq \frac{1}{(n-1)^2}(1{,}78)^{n-2}.$$

Hier kann D, da es quadratfrei ist, höchstens fünf lineare Primteiler haben. Schlimmstenfalls sind also die übrigen quadratisch. Also für $n \geqq 5$:

$$s \leqq 5 + \frac{n-5}{2} \quad \text{oder} \quad 2^{s-1} \leqq 2^4 \cdot 2^{\frac{n-5}{2}} = 2^4 (\sqrt{2})^{n-5}.$$

Also ist

$$f \geqq \frac{1}{n} \cdot \frac{1}{2^4} \cdot (1{,}78)^4 \cdot \left(\frac{1{,}78}{1{,}42}\right)^{n-5} \quad \text{bzw.} \quad h \geqq \frac{1}{(n-1)^2} \cdot \frac{1}{2^4} (1{,}78)^3 \left(\frac{1{,}78}{1{,}42}\right)^{n-5}.$$

Wegen $\frac{1{,}78}{1{,}42} > 1$ haben wir wieder unser Resultat.

Für $p = 3$ hatten wir

$$h \geqq \frac{1}{n} (1{,}15)^{n-1} \quad \text{bzw.} \quad h \geqq \frac{1}{(n-1)^2} (1{,}15)^{n-2}.$$

D hat höchstens 3 lineare, 3 quadratische, 8 kubische und 18 biquadratische Primfaktoren. Also gilt für $n \geqq 105$

$$s \leqq 32 + \frac{n-105}{5}, \qquad 2^{s-1} \leqq 2^{31} \cdot (\sqrt[5]{2})^{n-105} = 2^{31} \cdot (1{,}149)^{n-105}.$$

Also ist

$$f \geqq \frac{1}{n} \cdot \frac{1}{2^{31}} \cdot (1{,}15)^{104} \cdot \left(\frac{1{,}15}{1{,}149}\right)^{n-105} \quad \text{bzw.} \quad f \geqq \frac{1}{n} \cdot \frac{1}{2^{31}} (1{,}15)^{103} \left(\frac{1{,}15}{1{,}149}\right)^{n-105},$$

woraus wegen $\left(\frac{1{,}15}{1{,}149}\right) > 1$ unsere Behauptung folgt.

Satz. Die Richtigkeit der Riemannschen Vermutung vorausgesetzt, gilt für die Klassenzahl in imaginären Körpern, von linearen und quadratischen Diskriminanten abgesehen:

1. Für alle p und n gibt es nur endlich viele Körper vorgegebener Klassenzahl. Insbesondere kann es nur für $p = 3$ Körper mit der Klassenzahl 1 geben. (Wahrscheinlich nur einen.)

2. Für alle p und n gibt es nur endlich viele Körper, bei denen die Anzahl der Klassen im einzelnen Geschlecht einen vorgeschriebenen Wert hat. Insbesondere gibt es nur endlich viele Körper mit einklassigen Geschlechtern, und zwar nur für die Primzahlen $p = 3$, $p = 5$ und $p = 7$. Beispiele sind: $K(\sqrt{t^3 - t})$, $K(\sqrt{t^3 + t})$, $K(\sqrt{t^3 - 1})$.

§ 25.

Die reellen Charaktere.

Hilfssatz. Ist P eine Primfunktion und n ein beliebig vorgegebener Exponent, so existiert stets eine primitive Kongruenzwurzel $G \pmod P$ im Sinne Dedekinds, für welche

$$G^{|P|-1} \equiv 1 \pmod{P^n}.$$

Beweis. Der Satz ist für $n=1$ nach Dedekind richtig. Er sei bis zum Exponenten n bewiesen. Dann gibt es also eine primitive Kongruenzwurzel G, für welche

$$G^{|P|-1} \equiv (1 + HP^n)$$

ist. Dasselbe leistet dann jedes

$$G + XP^n.$$

Es ist nun:

$$\begin{aligned}(G + XP^n)^{|P|-1} &\equiv G^{|P|-1} + (|P|-1)XP^n \cdot G^{|P|-2} \pmod{P^{n+1}} \\ &\equiv G^{|P|-1} - XP^n G^{|P|-2} \pmod{P^{n-1}} \\ &\equiv 1 + (H - X \cdot G^{|P|-2})P^n \pmod{P^{n+1}}.\end{aligned}$$

Bestimmen wir nun X aus der Kongruenz

$$X \cdot G^{|P|-2} \equiv H \pmod{P},$$

so gilt für die primitive Kongruenzwurzel $G + XP^n$:

$$(G + XP^n)^{|P|-1} \equiv 1 \pmod{P^{n+1}}.$$

Nun sei K irgendeine primäre Funktion und $K = P_1^{n_1} P_2^{n_2} \dots P_r^{n_r}$ ihre Zerlegung in Primfunktionen. Wir setzen

$$M = P_1 P_2 \dots P_r.$$

Wenn nun $\Phi(K)$ die Anzahl der primen Restklassen modulo K bedeutet, ist nach Dedekind

$$\begin{aligned}\Phi(K) &= |P_1|^{n_1-1} |P_2|^{n_2-1} \dots |P_r|^{n_r-1} (|P_1|-1)(|P_2|-1) \dots (|P_r|-1) \\ &= p^l \Phi(M),\end{aligned}$$

wo p^l eine gewisse Potenz von p, $\Phi(M)$ dagegen, da M nur einfache Primfaktoren enthält, zu p prim ist.

Wir betrachten nun die Gruppe $\mathfrak{G}$ der primen Restklassen modulo K vom Grade $p^l \Phi(M)$.

Es seien $G_1, G_2, \dots, G_r$ primitive Kongruenzwurzeln modulo bzw. $P_1, P_2, \dots, P_r$, für welche

$$G_r^{|P_r|-1} \equiv 1 \pmod{P_r^{n_r}}.$$

Sind dann $a_1, a_2, \dots, a_r$ irgendwelche Zahlen (nicht im Sinne modulo p), so ist das System der Kongruenzen

$$(1) \qquad \begin{cases} X \equiv G_1^{a_1} \pmod{P_1^{n_1}} \\ X \equiv G_2^{a_2} \pmod{P_2^{n_2}} \\ \cdots\cdots\cdots \\ X \equiv G_r^{a_r} \pmod{P_r^{n_r}} \end{cases}$$

stets lösbar, und zwar liegen ersichtlich alle Lösungen in einer und nur einer Restklasse S modulo K. Ferner ändert sich, wegen $G^{|P_\nu|-1} \equiv 1 \pmod{P_\nu^{n_\nu}}$, S nicht, wenn die Zahlen a_ν um Vielfache von $|P_\nu| - 1$ vermehrt werden. Ebenso folgt aus $G_\nu^{a_\nu} \equiv G_\nu^{b_\nu} \pmod{P_\nu^{n_\nu}}$, da ja G_ν primitive Kongruenzwurzel ist, daß sich a_ν und b_ν nur um ein Vielfaches von $|P_\nu| - 1$ unterscheiden.

Lassen wir also die Zahlen a_ν das System der Werte $0 \leqq a_\nu \leqq |P_\nu| - 2$ durchlaufen, so erhalten wir lauter verschiedene Restklassen S in der Anzahl

$$(|P_1| - 1) \dots (|P_r| - 1) = \Phi(M).$$

Diese Restklassen bilden nun ersichtlich eine Gruppe $\mathfrak{G}_1$ vom Grade $\Phi(M)$, welche Untergruppe von $\mathfrak{G}$ ist.

Nennen wir nun S_ν jene Restklasse von $\mathfrak{G}_1$, deren Repräsentant X den Kongruenzen (1) genügt, wo $a_\mu = 0$ für $\mu \neq \nu$, dagegen $a_\mu = 1$ für $\mu = \nu$ ist, so bilden die Restklassen $S_1, S_2, \dots, S_r$, wie man leicht erkennt, eine Basis von $\mathfrak{G}_1$. Wir erhalten dann alle Restklassen von $\mathfrak{G}_1$ in der Form

$$S = S_1^{a_1} S_2^{a_2} \dots S_r^{a_r}, \qquad \text{wo} \qquad 0 \leqq a_\nu \leqq |P_\nu| - 2.$$

Da nun der Grad von $\mathfrak{G}$ den Wert $p^l \Phi(M)$ hat, und $\Phi(M)$ (das ist der Grad von $\mathfrak{G}_1$) prim ist zu p^l, läßt sich nach bekannten Sätzen $\mathfrak{G}$ darstellen als direktes Produkt:

$$\mathfrak{G} = \mathfrak{G}_1 \mathfrak{G}_2,$$

wo $\mathfrak{G}_2$ eine weitere Untergruppe von $\mathfrak{G}$ ist, und zwar den Grad p^l hat.

Jede Restklasse S aus $\mathfrak{G}$, d. h. jede prime Restklasse modulo K läßt sich also darstellen in der Form

$$S = S_1^{a_1} S_2^{a_2} \dots S_r^{a_r} \cdot T, \tag{2}$$

wo T eine Restklasse aus $\mathfrak{G}_2$ ist.

Jeder Charakter von $\mathfrak{G}$ hat also die Form

$$\chi(S) = \chi_1(S_1^{a_1} S_2^{a_2} \dots S_r^{a_r}) \cdot \chi_2(T).$$

Dabei ist χ_1 ein Charakter der Untergruppe $\mathfrak{G}_1$, χ_2 ein solcher von $\mathfrak{G}_2$. Nun hat $\mathfrak{G}_2$ den ungeraden Grad p^l, also ist der Hauptcharakter von $\mathfrak{G}_2$ ihr einziger reeller Charakter.

Soll also χ ein reeller Charakter von $\mathfrak{G}$ sein, so muß χ_2 der Hauptcharakter von $\mathfrak{G}_2$, χ_1 aber ein reeller Charakter von $\mathfrak{G}_1$ sein. Für reelle Charaktere ist also

$$\chi(S) = (\pm 1)^{a_1} (\pm 1)^{a_2} (\pm 1)^{a_3} \dots (\pm 1)^{a_r}, \tag{3}$$

wo also, wenn χ ein fester Charakter ist, jeder Primfunktion P_ν ein bestimmtes Vorzeichen ± 1 zugeordnet ist.

Sei nun Q das Produkt jener P_ν, denen in (3) ein negatives Zeichen, R das Produkt jener P_ν, denen ein positives Zeichen zukommt. Ferner sei A ein Repräsentant von S, B ein Repräsentant der Klasse T in (2). Dann ist

$$A \equiv G_\nu^{a_\nu} B \pmod{P_\nu^{n_\nu}}. \tag{3a}$$

Nun ist T eine Restklasse aus $\mathfrak{G}_2$ vom Grade p^l, also $T^{p^s} = 1$, wenn p^s der Exponent von T ist, der ja in p^l aufgehen muß. Also ist

$$\left.\begin{aligned} &B^{p^s} \equiv 1 \pmod{K} \\ &\text{und um so mehr} \\ &B^{p^s} \equiv 1 \pmod{P_\nu}. \end{aligned}\right\} \tag{4}$$

Wir betrachten nun den Exponenten von B modulo P_ν (also nur erste Potenz!). Einerseits muß er im Grade der Gruppe der primen Restklassen mod P_ν, also in $(|P_\nu| - 1)$ aufgehen, andererseits aber nach (4) in dem dazu primen p^s. Dieser Exponent muß also 1 sein. Demnach

$$B \equiv 1 \pmod{P_\nu}. \tag{5}$$

Aus (3a) und (5) folgt also

$$A \equiv G_\nu^{a_\nu} \pmod{P_\nu};$$

von nun an sei A primär.

Wegen $\left[\frac{G_\nu}{P_\nu}\right] = -1$ (dies folgt unmittelbar aus der Definition der primitiven Kongruenzwurzel) ist also

$$\left[\frac{A}{P_\nu}\right] = (-1)^{a_\nu}.$$

Also folgt

$$\chi(A) = \left[\frac{A}{Q}\right]$$

(Q Produkt aller P_ν, denen ein Minuszeichen entspricht).

Sei nun n der Grad von Q, μ der von A. Dann ist

$$\chi(A) = \left[\frac{A}{Q}\right] = \left(\frac{-1}{p}\right)^{n\mu}\left[\frac{Q}{A}\right] = \left(\left(\frac{-1}{p}\right)^n\right)^\mu\left[\frac{QR^2}{A}\right].$$

Setzen wir also

$$D = \left(\frac{-1}{p}\right)^n \cdot Q \cdot R^2,$$

so ist nach dem Ergänzungssatz $\chi(A) = \left[\frac{D}{A}\right]$.

Wenn nun A prim zu $K = QRN$ ist, ist es auch prim zu D und umgekehrt. Für die reellen L-Reihen finden wir also

$$L(s, \chi) = \sum_{\substack{\operatorname{sgn} A = 1 \\ (A,K)=1}} \frac{\chi(A)}{A^s} = \sum_{\substack{\operatorname{sgn} A = 1 \\ (A,D)=1}} \left[\frac{D}{A}\right] \frac{1}{A^s} = \prod_{\substack{\operatorname{sgn} P = 1 \\ (P,D)=1}} \frac{1}{1 - \left[\frac{D}{P}\right] \cdot P^{-s}}.$$

1. χ der Hauptcharakter. Dann ist $Q=1$, $n=0$, also $D=R^2$, und wir haben

$$(6)\qquad L(s,\chi)=\prod_{(P,D)=1}\frac{1}{1-|P|^{-s}}=\prod_{\nu=1}^{r}\left(1-\frac{1}{P_\nu^{\,s}}\right)\cdot\prod_{P}\frac{1}{1-|P|^{-s}}$$

$$=\frac{1}{1-p^{-(s-1)}}\cdot\prod_{\nu=1}^{r}\left(1-\frac{1}{|P_\nu|^s}\right).$$

2. χ ein vom Hauptcharakter verschiedener reeller Charakter. Wir setzen $D=D_1R^2$, wo also $D_1=\left(\frac{-1}{p}\right)^n Q$ und $|Q|>1$ quadratfrei ist. Dann ist D_1 Diskriminante eines quadratischen Körpers. Wegen $M=QR$ ist endlich D_1 prim zu R. Die in R aufgehenden verschiedenen Primfunktionen mögen $R_1, R_2, \ldots, R_\varkappa$ heißen. Dann ist

$$L(s,\chi)=\prod_{(P,D)=1}\frac{1}{1-\left[\frac{D}{P}\right]|P|^{-s}}=\prod_{\nu=1}^{\varkappa}\left(1-\left[\frac{D_1}{R_\nu}\right]|R_\nu|^{-s}\right)\cdot\prod_{(P,D_1)=1}\frac{1}{1-\left[\frac{D_1}{P}\right]|P|^{-s}}$$

$$=\prod_{\nu=1}^{\varkappa}\left(1-\left[\frac{D_1}{R_\nu}\right]\cdot|R_\nu|^{-s}\right)\cdot\sum_{\substack{\operatorname{sgn}A=1\\(A,D_1)=1}}{}'\left[\frac{D_1}{A}\right]\frac{1}{A^s}.$$

Also

$$(7)\qquad L(s,\chi)=\prod_{\nu=1}^{\varkappa}\left(1-\left[\frac{D_1}{R_\nu}\right]\cdot|R_\nu|^{-s}\right)(1-p^{-(s-1)})\cdot Z_{D_1}(s).$$

§ 26.

Die Anzahl der Primfunktionen gegebenen Grades in arithmetischen Progressionen.

Satz. Sei χ irgendein Charakter mod K. Dann besitzt $L(s,\chi)$ auf der Geraden $\Re(s)=1$ keine Nullstelle.

Beweis. 1. χ sei ein reeller Charakter. In (6) und (7) haben die Faktoren der Form $(1\pm|P|^{-s})$ nur Nullstellen auf $\Re(s)=0$. (6) hat keine Nullstelle. In (7) kürzen sich die Nullstellen des mittleren Faktors gegen die Pole von $Z(s)$. Ferner hat auch $Z_{D_1}(s)$ keine Nullstelle auf $\Re(s)=1$. Also hat $L(s,\chi)$ keine Nullstelle auf $\Re(s)=1$.

2. χ sei ein komplexer Charakter. Wir wenden das Beweisverfahren aus Landau, Handbuch der Lehre von der Verteilung der Primzahlen, S. 460, an.

Es ist

$$L(s,\chi)=L(s)=e^{\log L(s)}=e^{\sum_{m,P}{}'\frac{\chi(P^m)}{m|P|^{ms}}},$$

wo der Akzent am Summenzeichen bedeutet, daß über die zu K primen Primfunktionen P zu summieren ist.

Setzt man mit Landau $\chi(P^m) = e^{i\omega(P^m)}$, so ergibt sich wie dort, wenn $s = \sigma + it$ gesetzt ist (wo natürlich $\sigma > 1$),

$$|L(s,\chi)| = e^{\sum'_{m,P} \frac{\cos(\omega(P^m) - mt\log|P|)}{m|P|^{m\sigma}}}.$$

Aus der Ungleichung $\cos\varphi \geqq -\frac{3}{4} - \frac{1}{4}\cos 2\varphi$ findet man

$$|L(s)| \geqq e^{-\frac{3}{4}\sum'_{m,P}\frac{1}{m|P|^{ms}} - \frac{1}{4}\sum'_{m,P}\frac{\cos 2(\omega(P^m) - 2mt\log|P|)}{m|P|^{m\sigma}}}.$$

Hier ist

$$\sum'_{m,P}\frac{1}{m|P|^{m\sigma}} \leqq \sum_{m,P}\frac{1}{m|P|^{m\sigma}} = \log\prod_P \frac{1}{1-\frac{1}{P^s}} = -\log(1-p^{-(\sigma-1)}),$$

also

$$e^{-\frac{3}{4}\sum'_{m,P}\frac{1}{m|P|^{m\sigma}}} \geqq (1-p^{-(\sigma-1)})^{3/4},$$

und wie bei Landau

$$(1)\qquad e^{-\frac{1}{4}\sum'_{m,P}\frac{\cos(2\omega(P^m) - 2mt\log|P|)}{m|P|^{m\sigma}}} = \left| e^{-\frac{1}{4}\sum'_{m,P}\frac{(\chi(P^m))^2}{m|P|^{m(\sigma+2ti)}}} \right|.$$

Nun ist $(\chi(A))^2$ auch ein Charakter modulo K, und zwar sicher nicht der Hauptcharakter, da sonst $\chi(A)$ reell wäre, entgegen der Voraussetzung.

Im Exponenten rechts in (1) steht also auch der Logarithmus einer L-Reihe, wir nennen sie $L_1(s)$. Sie ist sicher nicht die des Hauptcharakters. Es wird

$$|L(s)| \geqq (1-p^{-(\sigma-1)})^{3/4} \cdot \frac{1}{(L_1(\sigma+2ti))^{1/4}}.$$

Also ist

$$\left|\frac{L(s)}{\sigma-1}\right| \geqq \left(\frac{1-p^{-(\sigma-1)}}{\sigma-1}\right)^{3/4} \frac{1}{((\sigma-1)L_1(\sigma+2ti))^{1/4}}.$$

Der in der Einleitung (I, § 1) genannten Arbeit von Kornblum entnehmen wir nun, daß $L(s)$ überall regulär ist, falls χ nicht der Hauptcharakter ist. Also hat $L_1(s)$ nirgends einen Pol.

Wir machen nun den Grenzübergang $\sigma \to 1$. Wegen

$$\lim_{\sigma=1}\frac{1-p^{-(\sigma-1)}}{\sigma-1} = \log p \neq 0$$

strebt die rechte Seite über alle Grenzen und somit auch die linke. $L(s)$ kann also in $1+it$ keine Nullstelle haben.

Nun ist wieder $L(s,\chi)$ periodisch mit der Periode $\frac{2\pi i}{\log p}$. Da die Gerade $\Re(s) = 1$ und ersichtlich auch die Halbebene $\Re(s) \geqq 1$ frei von

Nullstellen sind, schließen wir wieder, daß die obere Grenze θ der reellen Teile der Nullstellen aller zum Modul K gehörigen L-Reihen kleiner als 1 ist:

$$\theta < 1. \tag{2}$$

Nun gilt aber für Nichthauptcharaktere (nach Kornblum, S. 102), wenn m der Grad von K ist,

$$L(s,\chi) = \sum_{|A|<|K|} \frac{\chi(A)}{|A|^s} = \sum_{\nu=0}^{m-1} \frac{1}{p^{\nu s}} \Big(\sum_{|A|=p^\nu} \chi(A) \Big),$$

wo natürlich A primär und prim zu D ist. Setzen wir

$$\sigma_\nu(\chi) = \sum_{|A|=p^\nu} \chi(A) \quad \text{und} \quad p^s = z,$$

so wird für die Nullstellen von $L(s,\chi)$ die Gleichung gefunden

$$z^{m-1} + \sigma_1(\chi) z^{m-2} + \ldots + \sigma_{m-1}(\chi) = 0.$$

Ihre Wurzeln seien $\beta_1(\chi), \beta_2(\chi), \ldots, \beta_{m-1}(\chi)$. Dann ist wieder

$$L(s,\chi) = \prod_{\nu=1}^{m-1} (1 - \beta_\nu(\chi) \cdot p^{-s}).$$

Für den Hauptcharakter aber folgt aus dem vorigen Paragraphen

$$L(s,\chi_0) = \frac{1}{1-p^{-(s-1)}} \cdot \prod_{\nu=1}^{n} (1 - \beta_\nu(\chi_0)\, p^{-s}),$$

wo n eine gewisse ganze Zahl ist.

Wir numerieren nun die Charaktere: $\chi_0, \chi_1, \ldots, \chi_{\Phi(K)-1}$. χ_0 sei der Hauptcharakter. Dann ist

$$\log L(s,\chi) = \sum_{\nu=1}^{\infty} \frac{-\beta_1^\nu(\chi) - \beta_2^\nu(\chi) - \ldots - \beta_{m-1}^\nu(\chi)}{\nu \cdot p^{\nu s}} \quad \text{für } \chi \neq \chi_0, \tag{3}$$

$$\log L(s,\chi_0) = \sum_{\nu=1}^{\infty} \frac{p^\nu - \beta_1^\nu(\chi_0) - \ldots - \beta_n^\nu(\chi_0)}{\nu \cdot p^{\nu s}} \tag{4}$$

und allgemein

$$\log L(s,\chi) = \sum_{m,P}{}' \frac{\chi(P^m)}{m\,|P|^{m s}}. \tag{5}$$

Sei nun L Repräsentant irgendeiner zu K primen Restklasse. Wir bestimmen L_1 aus der Kongruenz

$$L L_1 \equiv 1 \pmod{K}$$

und bilden

$$(6) \qquad \sum_{\mu=1}^{\Phi(K)-1} \chi_\mu(L_1) \log L(s, \chi_\mu) = \sum_{m,P}{}' \frac{\sum_{\mu=0}^{\Phi(K)-1} \chi_\mu(L_1 P^m)}{m\,|P|^{ms}}.$$

Da nun

$$\sum_{\mu=0}^{\Phi(K)-1} \chi_\mu(F) = \begin{cases} \Phi(K), & \text{wenn } F \equiv 1 \pmod K, \\ 0 \quad , & \text{wenn } F \not\equiv 1 \pmod K, \end{cases}$$

ergibt sich

$$(7) \qquad \sum_{\mu=0}^{\Phi(K)-1} \chi_\mu(L_1) \log L(s, \chi_\mu) = \Phi(K) \sum_{\substack{P^m \equiv L \\ (\mathrm{mod}\ K)}} \frac{1}{m \cdot |P|^{ms}} = K_L(s).$$

Nennen wir nun $\pi_L(x, n)$ die Anzahl der Primfunktionen P, für welche $|P^n| = x$ und $P^n \equiv L \pmod K$ ist, so wird

$$(8) \qquad K_L(s) = \Phi(K) \cdot \sum_{\nu=1}^{\infty} \frac{\sum_{d|\nu} \frac{1}{d}\, \pi(p^\nu, d)}{p^{\nu s}}.$$

Andererseits ist nach (3) und (4)

$$(9) \qquad K_L(s) = \sum_{\nu=1}^{\infty} \frac{p^\nu - \Sigma \chi \beta^\nu}{\nu\, p^{\nu s}},$$

wo $\Sigma \chi \beta^\nu$ eine Summe über Charaktere und die ν-ten Potenzen der Wurzeln ist. Wegen (2) ist

$$|\beta^\nu| \leqq p^{\nu\theta}$$

und, da es nur endlich viele β und χ gibt,

$$(10) \qquad \Sigma \chi \beta^\nu = O(p^{\nu\theta}), \quad \text{wo } \theta < 1.$$

Aus (8) und (9) folgt aber

$$(11) \qquad \Phi(K) \sum_{d|\nu} \frac{\nu}{d}\, \pi_L(p^\nu, d) = p^\nu - \sum \chi \beta^\nu = p^\nu + O(p^{\theta\nu}).$$

Nun ist $\pi(p^\nu, d)$ höchstens gleich der Anzahl der Primfunktionen vom Grade $\frac{\nu}{d}$, also

$$\pi_L(p^\nu, d) < \frac{p^{\frac{\nu}{d}}}{\frac{\nu}{d}} = \frac{d}{\nu} \cdot p^{\frac{\nu}{d}}.$$

Somit ist

$$\sum_{\substack{d|\nu \\ d \geqq 2}} \frac{\nu}{d}\, \pi_L(p^\nu, d) \leqq \sum_{d=2}^{\nu} p^{\frac{\nu}{d}} = p^{\frac{\nu}{2}} + \sum_{d=3}^{\nu} p^{\frac{\nu}{d}} < p^{\frac{\nu}{2}} + \nu p^{\frac{\nu}{3}} = O(p^{\frac{\nu}{2}}).$$

Somit gilt, wenn wir $d = 1$ abspalten und $\pi_L(x, 1) = \pi_L(x)$ setzen, so daß also $\pi_L(x)$ gleich der Anzahl der Primfunktionen P mit $|P| = x$ und $P \equiv L \pmod K$ ist,

$$\Phi(K)\,\pi_L(p^\nu) = \frac{p^\nu}{\nu} + O\left(\frac{p^{\frac{\nu}{2}}}{\nu}\right) + O\left(\frac{p^{\theta\nu}}{\nu}\right).$$

Setzen wir nun also, und dies können wir tun, $\theta \geqq \frac{1}{2}$ voraus, so gilt

$$\pi_L(p^\nu) = \frac{p^\nu}{\nu \cdot \Phi(K)} + O\left(\frac{p^{\theta\nu}}{\nu}\right).$$

Also, wenn wieder x nur Werte p^ν annimmt,

$$\pi_L(x) = \frac{\log p}{\Phi(K)} \cdot \frac{x}{\log x} + O\left(\frac{x^\theta}{\log x}\right), \quad \text{wo } \tfrac{1}{2} \leqq \theta < 1. \tag{12}$$

Es gibt also von einem gewissen Grade an Primfunktionen jeden Grades in der arithmetischen Progression, und die Primfunktionen gegebenen Grades (primär) verteilen sich asymptotisch gleichmäßig auf die verschiedenen Progressionen gleichen Moduls. Dies ist eine wesentliche Verschärfung der von Kornblum und Landau gewonnenen Resultate.

(Eingegangen am 14. Oktober 1921.)

Zur Arithmetik der Polynome.

Von

E. Kamke in Münster i. W.

In dieser Arbeit[1]) gelten folgende Bezeichnungen: Für eine natürliche Zahl q und eine reelle Zahl α ist

$$e_q(\alpha) = e^{\frac{2\pi i \alpha}{q}}, \qquad e(\alpha) = e_1(\alpha);$$

$$P(u) = P_k(u) = a_k u^k + a_{k-1} u^{k-1} + \ldots + a_0$$

ist ein Polynom des Grades $k \geqq 1$ mit ganzen Zahlen als Koeffizienten; $\mathfrak{a}$ ist ein Intervall und $|\mathfrak{a}|$ seine Länge; $q_{\mathfrak{a}}$ ist bei $|\mathfrak{a}| < q$ die Anzahl der mod q in $\mathfrak{a}$ hineinfallenden Polynomwerte $P(u)$, wenn u ein vollständiges Restsystem mod q durchläuft.

Die Arbeit beschäftigt sich in erster Linie mit der Frage: Was läßt sich über $q_{\mathfrak{a}}$ sagen?

Für die Behandlung derartiger Fragen hat man eine Handhabe in folgendem von Herrn Weyl[2]) bewiesenen „Prinzip“:

Gilt bei einer Menge reeller Zahlen $\alpha_1, \alpha_2, \ldots$ für jede ganze Zahl $m \neq 0$ die Limesgleichung

$$\sum_{u=1}^{n} e(m\alpha_u) = o(n), \tag{1}$$

so sind die Zahlen α_u mod 1 *gleichmäßig dicht verteilt, d. h. die Anzahl der* mod 1 *in ein Intervall $\mathfrak{a}$ mit $|\mathfrak{a}| < 1$ hineinfallenden Zahlen $\alpha_1, \ldots, \alpha_n$ ist asymptotisch gleich $|\mathfrak{a}|\, n$.*

Dieser Satz nebst dem von Herrn Weyl gegebenen Beweis läßt sich, was bisher nicht bemerkt zu sein scheint, so abändern, daß er auf die

[1]) Dieselbe bildet einen Abschnitt meiner Habilitationsschrift, die Ostern 1922 der Philos. Fakultät der Universität Münster i. W. vorgelegen hat.

[2]) *Über die Gleichverteilung von Zahlen mod. Eins*, Math. Ann. 77 (1916), S. 313 bis 352; Satz 1.

vorliegende Frage anwendbar ist und unter gewissen Einschränkungen für α nicht nur $q_\alpha \sim |\alpha|$, sondern auch eine Abschätzung des Fehlers $q_\alpha - |\alpha|$ liefert, sofern eine der Summe (1) entsprechende Summe scharf genug abgeschätzt ist.

Diese abzuschätzende Summe lautet aber

$$S = S(q, P) = \sum_{u=0}^{q-1} e_q(P(u)), \tag{2}$$

und über sie ist durch die Herren Hardy und Littlewood[3]) bereits bekannt, daß bei $d = (q, a_k)$ für jedes $\varepsilon > 0$ eine solche Zahl $A = A(k, d, \varepsilon)$ vorhanden ist, daß

$$|S| < A q^{1-2^{1-k}+\varepsilon} \tag{3}$$

ist. Dieses Ergebnis wird im § 1 insofern verschärft, als dort gezeigt wird, daß d durch $(q, a_k, \ldots, a_1)$ ersetzt werden kann. Im § 2 wird die entsprechende Abschätzung für Polynome zweier Veränderlicher durchgeführt und im § 3 dann mit dem modifizierten Prinzip $q_\alpha - |\alpha|$ abgeschätzt.

Mit $q_\alpha - |\alpha|$ ist natürlich auch die Anzahl der *einer* Restklasse mod q angehörenden Polynomwerte $P(u)$ abgeschätzt. In § 4 wird die so erhaltene Abschätzung auf völlig elementarem Wege erheblich verschärft.

§ 5 zeigt die Bedeutung der modifizierten Abschätzung (3) für das Waringsche Problem.

§ 1.

Verschärfung einer Abschätzung.

In den §§ 1—3 sei für natürliche Zahlen $k \geqq 1$

$$L = L(k) = \frac{1}{2^{k-1}}.$$

Satz 1. *Es sei S durch (2) erklärt, es bedeute $T(q)$ die Anzahl der Teiler von q, und es sei*[4])

$$\Delta = (q, a_k, a_{k-1}, \ldots, a_2).$$

Dann ist

$$|S| \begin{cases} \leqq k\, T(q)\, \Delta^L q^{1-L} & \text{für } \Delta \mid a_1, \\ = 0 & \text{für } \Delta \nmid a_1. \end{cases} \tag{4}$$

[3]) *Some problems of „Partitio Numerorum"*; I: *A new solution of Waring's Problem*, Nachr. v. d. K. Gesellschaft d. Wissensch. zu Göttingen, Mathem.-physik. Klasse, 1920, S. 33—54, Lemma 1; zwar erscheint dort die Behauptung nicht in der obigen Formulierung, ist aber im Beweise enthalten. Vgl. hierzu auch Landau: *Zum Waringschen Problem*, Math. Zeitschr. 12 (1922), S. 219—247, Hilfssatz 6, Vorbemerkung und Beweis.

[4]) Für $k = 1$ sei $\Delta = q$.

Anmerkung. Für

$$\delta = (q, a_k, a_{k-1}, \ldots, a_1)$$

folgt hieraus insbesondere

$$|S| \leqq k\,T(q)\,\delta^{L(k)} q^{1-L(k)}. \tag{5}$$

Wegen $T(q) = O(q^\varepsilon)$ ist hierin (3) enthalten, und es ergibt sich für alle Polynome $P(u)$ mit $(a_k, \ldots, a_1) = 1$ die Existenz einer solchen Zahl $B = B(k, \varepsilon)$ für jedes $\varepsilon > 0$, daß

$$|S| < B q^{1-2^{1-k}+\varepsilon} \tag{6}$$

ist.

Beweis[5]. Für $k = 1$ ist offenbar

$$|S| = \left| \sum_{u=0}^{q-1} e^{\frac{2\pi i a_1 u}{q}} \right| = \begin{cases} q & \text{für } q \mid a_1, \\ 0 & \text{für } q \nmid a_1, \end{cases}$$

also die Behauptung richtig.

Um den zweiten Teil von (4) für beliebiges k zu beweisen, setzen wir

$$q = \Delta Q, \qquad u = Q\mu + \bar{\mu} \quad \text{mit } 0 \leqq \bar{\mu} < Q.$$

Wegen $\Delta \mid a_k, \ldots, a_2$ ist dann

$$\begin{aligned} e_q(P(u)) &= e_{\Delta Q}\{a_k(Q\mu + \bar{\mu})^k + \ldots + a_1(Q\mu + \bar{\mu}) + a_0\} \\ &= e_{\Delta Q}\{P(\bar{\mu}) + a_1 Q\mu\} = e_{\Delta Q}(P(\bar{\mu}))\, e_\Delta(a_1\mu), \end{aligned}$$

also

$$S = \sum_{\bar{\mu}=0}^{Q-1} e_{\Delta Q}(P(\bar{\mu})) \sum_{\mu=0}^{\Delta-1} e_\Delta(a_1\mu) = 0,$$

da die innere Summe wegen $\Delta \nmid a_1$ nach dem für $k = 1$ Gezeigten den Wert 0 hat.

Es bleibt noch der erste Teil von (4) für $k \geqq 2$ zu beweisen. Wir können annehmen, dieser Teil der Behauptung, und damit (5), sei schon für $k - 1$ bewiesen. Es ist

$$|S|^2 = \sum_{u} \sum_{h} e_q(P(u) - P(h)),$$

wo u, h je ein vollständiges Restsystem mod q durchlaufen. Wird $u = i + h$ gesetzt, so durchlaufen i, h gleichzeitig vollständige Restsysteme mit u, h. Daher ist

$$|S|^2 \leqq \sum_{i=0}^{q-1} \left| \sum_{h} \right|, \tag{7}$$

[5]) Der Beweis ist eine Verallgemeinerung eines Beweises (verschieden von dem in Fußnote 3 erwähnten), den Herr Landau für den Fall, daß in der Abschätzung nur $d = (q, a_k)$ statt Δ in Betracht gezogen wird, am 7. 4. 1921 in einem Briefe an Herrn Hardy gegeben und mir freundlicherweise ebenfalls mitgeteilt hat.

wo

$$\sum_h = \sum_{h=0}^{q-1} e_q\left(\sum_{\varkappa=0}^{k-1} h^\varkappa \sum_{\lambda=\varkappa+1}^{k} a_\lambda \binom{\lambda}{\varkappa} i^{\lambda-\varkappa}\right)$$

ist. Hier steht in der großen Klammer ein Polynom $(k-1)$-ten Grades von h. Nach der für $k-1$ als richtig angenommenen Abschätzung (5) ist daher

$$|\sum_h| \leqq (k-1)\, T(q)\, \delta_i^{L(k-1)} q^{1-L(k-1)}, \tag{8}$$

wo

$$\delta_i = \left(q, a_k \binom{k}{k-1} i, \sum_{\lambda=k-1}^{k} a_\lambda \binom{\lambda}{k-2} i^{\lambda-k+2}, \sum_{\lambda=k-2}^{k} a_\lambda \binom{\lambda}{k-3} i^{\lambda-k+3}, \ldots, \sum_{\lambda=2}^{k} a_\lambda \binom{\lambda}{1} i^{\lambda}\right.$$

ist.

Da

$$(xy, z, \ldots) \leqq (x, z, \ldots)(y, z, \ldots)$$

ist, ergibt sich

$$\begin{aligned}\delta_i &\leqq (q, k, \ldots)(q, a_k i, \ldots)\\ &\leqq k\,(q, a_k i, \sum_{\lambda=k-1}^{k}, \sum_{\lambda=k-2}^{k}, \ldots, \sum_{\lambda=2}^{k}).\end{aligned}$$

Da $a_k i$ als einzelnes Element in der Klammer vorkommt, kann in jeder der nach ihm folgenden Summen das letzte Glied fortgelassen werden, da es ein Vielfaches von $a_k i$ ist. Man hat also

$$\delta_i \leqq k\left(q, a_k i, a_{k-1}(k-1)\, i, \sum_{\lambda=k-2}^{k-1}, \sum_{\lambda=k-3}^{k-1}, \ldots, \sum_{\lambda=2}^{k-1}\right),$$

mithin, wie oben,

$$\delta_i \leqq k(k-1)\left(q, a_k i, a_{k-1} i, \sum_{\lambda=k-2}^{k-1}, \sum_{\lambda=k-3}^{k-1}, \ldots, \sum_{\lambda=2}^{k-1}\right).$$

Nun kann wieder das letzte Glied jeder Summe fortgelassen werden. Die Wiederholung des Verfahrens ergibt schließlich

$$\begin{aligned}\delta_i &\leqq k!\,(q, a_k i, a_{k-1} i, \ldots, a_2 i)\\ &\leqq k!\,(q, a_k, \ldots, a_2)(q, i) \leqq k^{2^{k-2}} \Delta(q, i).\end{aligned}$$

Daher folgt aus (7) und (8)

$$|S|^2 \leqq k^2\, T(q)\, \Delta^{L(k-1)} q^{1-L(k-1)} \sum_{i=0}^{q-1}(q, i).$$

Hierbei ist

$$\sum_{i=0}^{q-1}(q, i) \leqq \sum_{t \mid q} t \sum_{\nu=1}^{q/t} 1 = q \sum_{t \mid q} 1 = q\, T(q).$$

Mithin ist wegen $L(k-1) = 2\,L(k)$

$$|S|^2 \leqq k^2\, T^2(q)\, \Delta^{2L(k)} q^{2-2L(k)},$$

woraus die Behauptung folgt.

§ 2.

Ausdehnung der Abschätzung auf Polynome zweier Veränderlicher.

Ähnliche Abschätzungen wie in § 1 für Polynome einer Veränderlichen lassen sich auch für Polynome mehrerer Veränderlicher geben. Wir beschränken uns hier auf zwei Veränderliche und beweisen den

Satz 2. *Es sei*

$$P(u, v) = \sum_{0 \leq \varkappa + \lambda \leq k} a_{\varkappa\lambda} u^{\varkappa} v^{\lambda}$$

ein Polynom höchstens k-ten Grades; es sei

$$R = R(q, P) = \sum_{u=0}^{q-1} \sum_{v=0}^{q-1} e_q(P(u, v))$$

und

$$\Delta = (q, \ldots, a_{\varkappa\lambda}, \ldots)_{(\varkappa+\lambda \geqq 2)},$$

d. h. der größte gemeinsame Teiler von q und allen $a_{\varkappa\lambda}$ mit $\varkappa + \lambda \geqq 2$. Dann ist

$$R \begin{cases} \leqq (k!)^2 T(q) \Delta^L q^{2-L} & \text{für } \Delta \mid (a_{10}, a_{01}), \\ = 0 & \text{für } \Delta \nmid (a_{10}, a_{01}). \end{cases} \tag{9}$$

Anmerkung. Hieraus folgt insbesondere, wenn δ den größten gemeinsamen Teiler von q und allen $a_{\varkappa\lambda}$ mit $\varkappa + \lambda \geqq 1$ bezeichnet.

$$R \leqq (k!)^2 T(q) \delta^{L(k)} q^{2-L(k)}. \tag{10}$$

Beweis. Für $k = 1$ ist (9) richtig, da dann

$$R = \sum_{u=0}^{q-1} \sum_{v=0}^{q-1} e_q(a_{10} u + a_{01} v + a_{00})$$

$$= e_q(a_{00}) \sum_{u=0}^{q-1} e_q(a_{10} u) \sum_{v=0}^{q-1} e_q(a_{01} v)$$

ist, hier offenbar nur dann *beide* Summen $= 0$ sind, wenn $\Delta = q \mid (a_{10}, a_{01})$ ist, und da in diesem Falle

$$R = q^2 = \Delta q.$$

Um den zweiten Teil von (9) für beliebiges k zu beweisen, setzen wir

$$q = \Delta Q, \qquad u = Q\mu - \mu, \qquad v = Q\nu - \nu.$$

Dann ist wegen $\Delta \mid a_{\varkappa\lambda}$ für $\varkappa + \lambda \geqq 2$

$$e_q(P(u, v)) = e_{\Delta Q}(P(\bar{\mu}, \bar{\nu}))\, e_{\Delta}(a_{10}\mu + a_{01}\nu),$$

also

$$R \leqq \sum_{\mu=0}^{Q-1} \sum_{\nu=0}^{Q-1} \sum_{u=0}^{\Delta-1} \sum_{v=0}^{\Delta-1} e_{\Delta}(a_{10}\mu + a_{01}\nu) = 0,$$

da die innere Doppelsumme wegen $\Delta \not\equiv (a_{10}, a_{01})$ nach dem für $k=1$ Gezeigten den Wert 0 hat.

Es bleibt noch der erste Teil von (9) für $k \geqq 2$ zu beweisen. Wir nehmen an, dieser Teil der Behauptung, und damit (10), sei bereits bis $k-1$ bewiesen. Es ist

$$|R|^2 = \sum_{u,v,h,l}{}' e_q\Big(\sum_{0 \leqq \varkappa+\lambda \leqq k} a_{\varkappa\lambda}(u^\varkappa v^\lambda - h^\varkappa l^\lambda)\Big),$$

wo u, v, h, l je ein vollständiges Restsystem mod q durchlaufen. Wird $u = i+h$, $v = j+l$ gesetzt, so durchlaufen zugleich mit jenen Zahlen auch i, j, h, l vollständige Restsysteme. Daher ist

$$|R|^2 \leqq \sum_{i=0}^{q-1}\sum_{j=0}^{q-1} \Big|\sum_{k=0}^{q-1}\sum_{l=0}^{q-1} e_q(\Sigma)\Big|, \tag{11}$$

wo

$$\Sigma = \sum_{0 \leqq \varkappa+\lambda \leqq k} \Big\{ a_{\varkappa\lambda} \sum_{\varrho=0}^{\varkappa}\sum_{\sigma=0}^{\lambda} h^\varrho l^\sigma \binom{\varkappa}{\varrho}\binom{\lambda}{\sigma} i^{\varkappa-\varrho} j^{\lambda-\sigma} - a_{\varkappa\lambda} h^\varkappa l^\lambda \Big\}$$

$$= \sum_{0 \leqq \varrho+\sigma \leqq k} h^\varrho l^\sigma \Big\{ \sum_{\substack{\varkappa \geqq \varrho,\ \lambda \geqq \sigma \\ \varkappa+\lambda \leqq k}} a_{\varkappa\lambda} \binom{\varkappa}{\varrho}\binom{\lambda}{\sigma} i^{\varkappa-\varrho} j^{\lambda-\sigma} - a_{\varrho\sigma} \Big\}$$

ist. Hier hebt sich in der Klammer das Glied mit $\varkappa = \varrho$, $\lambda = \sigma$ gegen $a_{\varrho\sigma}$ fort. Mithin kommen in der Klammer nur Glieder mit $\varkappa + \lambda \geqq \varrho + \sigma + 1$ vor, und daher wegen $\varkappa + \lambda \leqq k$ Glieder mit $\varrho + \sigma = k$ nicht vor. Es ist daher

$$\Sigma = \sum_{0 \leqq \varrho+\sigma \leqq k-1} h^\varrho l^\sigma \sum_{\substack{\varkappa \geqq \varrho,\ \lambda \geqq \sigma \\ \varrho+\sigma+1 \leqq \varkappa+\lambda \leqq k}} a_{\varkappa\lambda} \binom{\varkappa}{\varrho}\binom{\lambda}{\sigma} i^{\varkappa-\varrho} j^{\lambda-\sigma}$$

ein Polynom höchstens $(k-1)$-ten Grades. Daher ist auf die innere Doppelsumme von (11) die Abschätzung (10) anwendbar, also wegen $L(k-1) = 2L(k)$

$$|R|^2 \leqq ((k-1)!)^2 T(q)\, q^{2-2L(k)} \sum_{i=0}^{q-1}\sum_{j=0}^{q-1} \delta_{ij}^{2L(k)}, \tag{12}$$

wo

$$\delta_{ij} = \Big(q, \ldots, \sum_{\substack{\varkappa \geqq \varrho,\ \lambda \geqq \sigma \\ \varrho+\sigma+1 \leqq \varkappa+\lambda \leqq k}} a_{\varkappa\lambda} \binom{\varkappa}{\varrho}\binom{\lambda}{\sigma} i^{\varkappa-\varrho} j^{\lambda-\sigma}, \ldots\Big)$$

ist und in dieser Klammer alle für $1 \leqq \varrho + \sigma \leqq k-1$ sich ergebenden Summen aufzuführen sind. Die Summen sollen in der Klammer so geordnet werden, daß die Summen mit demselben Wert von $\varrho + \sigma$ zusammenstehen. Wir schreiben dann

$$\delta_{ij} = (q, \ldots, \sum_{\substack{\varkappa+\lambda=k \\ (\varrho+\sigma=k-1)}}, \ldots, \sum_{\substack{k-1 \leqq \varkappa+\lambda \leqq k \\ (\varrho+\sigma=k-2)}}, \ldots, \sum_{\substack{k-2 \leqq \varkappa+\lambda \leqq k \\ (\varrho+\sigma=k-3)}}, \ldots, \sum_{\substack{2 \leqq \varkappa+\lambda \leqq k \\ (\varrho+\sigma=1)}}, \ldots), \tag{13}$$

wo hinter jedem Summenzeichen

$$A_{\varkappa\lambda}(\varrho,\sigma)=a_{\varkappa\lambda}\binom{\varkappa}{\varrho}\binom{\lambda}{\sigma}i^{\varkappa-\varrho}j^{\lambda-\sigma} \tag{14}$$

zu denken und in jeder Summe bei festem ϱ, σ nach wie vor nur über die Zahlen $\varkappa \geqq \varrho$, $\lambda \geqq \sigma$ mit der außerdem für $\varkappa+\lambda$ angegebenen Einschränkung zu summieren ist.

Um nun δ_{ij} abzuschätzen, zeigen wir zunächst, daß bei festem $K\,(3 \leqq K \leqq k)$ und festen ϱ, σ mit $1 \leqq \varrho+\sigma \leqq K-2$

$$\begin{aligned}(15)\quad &(K-\varrho-\sigma)\sum_{\substack{\varkappa\geqq\varrho,\ \lambda\geqq\sigma\\ \varkappa+\lambda=K}} A_{\varkappa\lambda}(\varrho,\sigma)\\ &=(\varrho+1)i\sum_{\substack{\varkappa\geqq\varrho+1,\ \lambda\geqq\sigma\\ \varkappa+\lambda=K}} A_{\varkappa\lambda}(\varrho+1,\sigma)+(\sigma+1)j\sum_{\substack{\varkappa\geqq\varrho,\ \lambda\geqq\sigma+1\\ \varkappa+\lambda=K}} A_{\varkappa\lambda}(\varrho,\sigma+1)\end{aligned}$$

ist. In der Tat ist die rechte Seite hiervon wegen (14), wenn wir von der ersten Summe das Glied mit $\lambda=\sigma$, von der zweiten das Glied mit $\varkappa=\varrho$ besonders aufschreiben,

$$a_{K-\sigma,\sigma}\binom{K-\sigma}{\varrho}(K-\sigma-\varrho)i^{K-\varrho-\sigma}+\sum_{\substack{\varkappa\geqq\varrho+1,\ \lambda\geqq\sigma+1\\ \varkappa+\lambda=K}}{}' a_{\varkappa\lambda}\binom{\varkappa}{\varrho}(\varkappa-\varrho)\binom{\lambda}{\sigma}i^{\varkappa-\varrho}j^{\lambda-\sigma}$$

$$+\sum_{\substack{\varkappa\geqq\varrho+1,\ \lambda\geqq\sigma+1\\ \varkappa+\lambda=K}}{}' a_{\varkappa\lambda}\binom{\varkappa}{\varrho}\binom{\lambda}{\sigma}(\lambda-\sigma)i^{\varkappa-\varrho}j^{\lambda-\sigma}+a_{\varrho,K-\varrho}\binom{K-\varrho}{\sigma}(K-\varrho-\sigma)j^{K-\varrho-\sigma},$$

und nach Vereinigung der beiden mittleren Summen steht bei Beachtung von $\varkappa+\lambda=K$ die linke Seite von (15) da.

Aus (13) folgt, wenn wir die Summen aufspalten und noch ganzzahlige Faktoren hinzufügen,

$$\begin{aligned}\delta_{ij}\leqq(q,\ldots,&\sum_{\substack{\varkappa+\lambda=k\\ (\varrho+\sigma=k-1)}},\ldots,\ 2!\sum_{\substack{\varkappa+\lambda=k\\ (\varrho+\sigma=k-2)}}+2!\sum_{\substack{\varkappa+\lambda=k-1}},\ldots,\ 3!\sum_{\substack{\varkappa+\lambda=k\\ (\varrho+\sigma=k-3)}}+3!\sum_{\substack{k-2\leqq\varkappa+\lambda\leqq k-1}},\ldots\\ &\ldots,(k-1)!\sum_{\substack{\varkappa+\lambda=k\\ (\varrho+\sigma=1)}}+(k-1)!\sum_{\substack{2\leqq\varkappa+\lambda\leqq k-1}},\ldots).\end{aligned} \tag{16}$$

Hierin können die ersten Bestandteile der aufgespaltenen Summen gestrichen werden. Denn (15) besagt, daß sich jede Summe $(k-1)!\sum_{\substack{\varkappa+\lambda=k\\ (\varrho+\sigma=1)}}$ aus zwei Summen der Form $(k-2)!\sum_{\substack{\varkappa+\lambda=k\\ (\varrho+\sigma=2)}}$ linear und ganzzahlig komponieren läßt; ebenso jede dieser Summen aus zwei Summen der Form $(k-3)!\sum_{\substack{\varkappa+\lambda=k\\ (\varrho+\sigma=3)}}$; usw.; schließlich jede der Summen $2!\sum_{\substack{\varkappa+\lambda=k\\ (\varrho+\sigma=k-2)}}$ aus zwei Summanden der Form $\sum_{\substack{\varkappa+\lambda=k\\ (\varrho+\sigma=k-1)}}$; d. h. jede der genannten Summen läßt sich linear und ganzzahlig komponieren aus Summen der Form $\sum_{\substack{\varkappa+\lambda=k\\ (\varrho+\sigma=k-1)}}$. Da die

Summen dieser letzten Art sämtlich als Elemente der Klammer in (16) vorkommen, können in der Klammer alle andern vorstehend genannten Summen gestrichen werden, so daß wir erhalten

$$\delta_{ij}' \leqq (q, \ldots, \sum_{\substack{\varkappa+\lambda=k \\ (\varrho+\sigma=k-1)}}, \ldots, \; 2! \sum_{\substack{\varkappa+\lambda=k-1 \\ (\varrho+\sigma=k-2)}}, \ldots, \; 3! \sum_{\substack{k-2 \leqq \varkappa+\lambda \leqq k-1 \\ (\varrho+\sigma=k-3)}}, \ldots, \; (k-1)! \sum_{\substack{2 \leqq \varkappa+\lambda \leqq k-1 \\ (\varrho+\sigma=1)}}, \ldots),$$

also, wenn der höchste Faktor jeder Fakultät herausgezogen wird und die Summen wieder aufgespalten werden,

$$\delta_{ij} \leqq (k-1)!\,(q, \ldots, \sum_{\substack{\varkappa+\lambda=k \\ (\varrho+\sigma=k-1)}}, \ldots, \sum_{\substack{\varkappa+\lambda=k-1 \\ (\varrho+\sigma=k-2)}}, \ldots, \; 2! \sum_{\substack{\varkappa+\lambda=k-1 \\ (\varrho+\sigma=k-3)}} + 2! \sum_{\substack{\varkappa+\lambda=k-2 \\ (\varrho+\sigma=k-3)}}, \ldots$$

$$3! \sum_{\substack{\varkappa+\lambda=k-1 \\ (\varrho+\sigma=k-4)}} + 3! \sum_{\substack{k-3 \leqq \varkappa+\lambda \leqq k-2 \\ (\varrho+\sigma=k-4)}}, \ldots, \; (k-2)! \sum_{\substack{\varkappa+\lambda=k-1 \\ (\varrho+\sigma=1)}} + (k-2)! \sum_{\substack{2 \leqq \varkappa+\lambda \leqq k-2 \\ (\varrho+\sigma=1)}}, \ldots).$$

Hierauf wird (15) mit $K = k-1$ angewendet. Dann ergibt sich nach dem oben stehenden Muster, daß sich der erste Bestandteil der aufgespaltenen Summen linear und ganzzahlig komponieren läßt aus den Summen der Form $\sum_{\substack{\varkappa+\lambda=k-1 \\ (\varrho+\sigma=k-2)}}$, also gestrichen werden kann. Wird wieder der höchste Faktor jeder Fakultät herausgezogen und das Verfahren in der geschilderten Weise fortgesetzt, so gelangt man schließlich zu

$$(17) \qquad \delta_{ij} \leqq \prod_{n=2}^{k-1} n!\,(q, \ldots, \sum_{\substack{\varkappa+\lambda=k \\ (\varrho+\sigma=k-1)}}, \ldots, \sum_{\substack{\varkappa+\lambda=k-1 \\ (\varrho+\sigma=k-2)}}, \ldots, \sum_{\substack{\varkappa+\lambda=2 \\ (\varrho+\sigma=1)}}, \ldots).$$

Hierin ist, da auch stets $\varkappa \geqq \varrho$, $\lambda \geqq \sigma$ ist, jede der vorkommenden Summen wegen (14) von der Gestalt

$$\sum_{\varkappa+\lambda=\varrho+\sigma+1} A_{\varkappa\lambda}(\varrho, \sigma) = A_{\varrho,\sigma+1}(\varrho, \sigma) + A_{\varrho+1,\sigma}(\varrho, \sigma)$$
$$= a_{\varrho,\sigma+1}(\sigma+1)j + a_{\varrho+1,\sigma}(\varrho+1)i.$$

Da in (17) alle Zahlenpaare ϱ, σ mit $1 \leqq \varrho + \sigma \leqq k-1$ vorkommen, ist mithin

$$\delta_{ij} \leqq (k!)^{2^{k-2}}(q, \ldots, a_{\varrho,\sigma+1}(\sigma+1)j + a_{\varrho+1,\sigma}(\varrho+1)i, \ldots),$$

wobei hierin alle Gliederkomplexe mit $1 \leqq \varrho + \sigma \leqq k-1$ aufzuführen sind.

Daher folgt nun aus (12)

$$(18) \qquad |R|^2 \leqq (k!)^3 T(q) A^{2L(k)} q^{2-2L(k)} \sum_{i,j}',$$

wo

$$\sum_{i,j}' = \sum_{i=0}^{q-1} \sum_{j=0}^{q-1}' \left(\frac{q}{A}, \ldots, (\sigma+1)^{\frac{a_{\varrho,\sigma+1}}{A}} j + (\varrho+1)^{\frac{a_{\varrho+1,\sigma}}{A}} i, \ldots\right)$$

ist. Hier ist

$$(19) \qquad \sum_{i,j}' \leqq \sum_{t}^{q} t \cdot N,$$

wo N die Anzahl der i, j $(0 \leqq i, j < q)$ ist, für welche bei festem t die sämtlichen für $1 \leqq \varrho + \sigma \leqq k-1$ aufgeschriebenen Kongruenzen

$$(\sigma+1)\frac{a_{\varrho,\sigma+1}}{\Delta} j + (\varrho+1)\frac{a_{\varrho+1,\sigma}}{\Delta} i \equiv 0 \pmod{t} \tag{20}$$

erfüllt sind. Die Anzahl der mod t inkongruenten Lösungen i, j dieses Systems ist bekanntlich, wenn e_1, e_2 die Elementarteiler des Systems bedeuten,

$$(e_1, t)(e_2, t) \leqq (e_1, t)\, t,$$

also die Anzahl aller Lösungen i, j von (20)

$$N \leqq \frac{q^2}{t^2}(e_1, t)\, t = \frac{q^2}{t}(e_1, t). \tag{21}$$

Der Elementarteiler e_1 ist der größte gemeinsame Teiler aller Koeffizienten des Systems (20), also, da in ihm alle $a_{\varrho\sigma}$ mit $2 \leqq \varrho + \sigma \leqq k$ vorkommen, auf Grund der Definition von Δ

$$(e_1, t) = \left(t, \ldots, \sigma\frac{a_{\varrho\sigma}}{\Delta}, \ldots\right) \leqq k!\left(\frac{q}{\Delta}, \ldots, \frac{a_{\varrho\sigma}}{\Delta}, \ldots\right) = k!$$

Daher ist nach (19) und (21)

$$\sum_{i,j} \leqq \sum_{t \mid \frac{q}{i}} t\frac{q^2}{t} k! \leqq k!\, q^2\, T(q),$$

also nach (18)

$$|R|^2 \leqq (k!)^4 T^2(q)\, \Delta^{2L(k)} q^{4-2L(k)},$$

woraus die Behauptung folgt.

§ 3.

Das Weylsche Prinzip und seine Anwendung.

Nach dem Beweisverfahren Herrn Weyls zu seinem Satz 1 läßt sich durch geeignete Abänderung folgender Satz gewinnen.

Satz 3. *Es seien* γ $(0 < \gamma < 1)$ *sowie* $\alpha_1, \ldots, \alpha_n$ *reelle Zahlen; es sei* $\mathfrak{i}$ *ein Intervall, dessen Länge* $|\mathfrak{i}|$ *der Ungleichung*

$$n^{\gamma-1} \leqq |\mathfrak{i}| \leqq 1 - n^{\gamma-1} \tag{22}$$

genügt; es sei $J(n)$ *die Anzahl der* mod 1 *in* $\mathfrak{i}$ *liegenden Zahlen* $\alpha_1, \ldots, \alpha_n$. *Dann ist für* $p = (10n)^5$

$$\left|J(n) - n|\mathfrak{i}|\right| < 8\sum_{\varkappa=1}^{p}\frac{1}{\varkappa}\left|\sum_{h=1}^{n} e(\varkappa\alpha_h)\right| + 2n^{\gamma}. \tag{23}$$

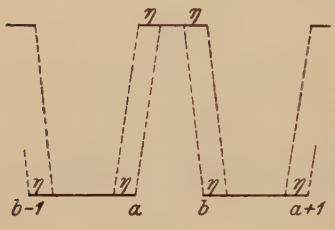
Beweis. Der Anfangspunkt des Intervalls i sei a, der Endpunkt b. Es werde eine reelle Funktion $f(x)$ mit der Periode 1 definiert durch

$$f(x) = \begin{cases} 1 & \text{für } a \leqq x \leqq b, \\ 0 & \text{für } b < x < a+1. \end{cases}$$

Es sei

$$\eta = \frac{1}{2} n^{\gamma-1}. \tag{24}$$

Wegen (22) ist 2η sicher nicht größer als jede der in der graphischen Darstellung von $f(x)$ vorkommenden zusammenhängenden Strecken. Es werden nun die oberen bzw. unteren zusammenhängenden Strecken beiderseitig um η verkürzt und die benachbarten Endpunkte in jedem Fall geradlinig verbunden. Die so entstehenden Linienzüge mögen die Funktionen $f_1(x)$ bzw. $f_2(x)$ definieren. Diese sind stetig, haben die Periode 1, und es ist



$$f_1(x) \leqq f(x) \leqq f_2(x).$$

Da nun offenbar

$$J(n) - n\,|\mathfrak{i}| = \sum_{h=1}^{n} \left\{ f(\alpha_h) - \int_0^1 f(x)\,dx \right\}$$

ist, so folgt, wenn zur Abkürzung

$$\mathfrak{I} = J(n) - n\,|\mathfrak{i}| \tag{25}$$

gesetzt wird,

$$\begin{cases} \mathfrak{I} \geqq \sum_{h=1}^{n} \left\{ f_1(\alpha_h) - \int_0^1 f_1(x)\,dx \right\} - n\eta, \\ \mathfrak{I} \leqq \sum_{h=1}^{n} \left\{ f_2(\alpha_h) - \int_0^1 f_2(x)\,dx \right\} + n\eta. \end{cases} \tag{26}$$

Es werden nun die Fourierentwicklungen von $f_1(x)$ und $f_2(x)$ gebildet. Die Fourierkoeffizienten von $f_1(x)$ seien $a_\varkappa, b_\varkappa$. Dann ist für $\varkappa = 1, 2, \ldots$

$$\frac{1}{2} a_\varkappa = \int_0^1 f_1(x) \cos 2\pi\varkappa x\,dx = \int_a^{a+\eta} + \int_{a+\eta}^{b-\eta} + \int_{b-\eta}^{b}.$$

Dabei ist

$$\left| \int_{a+\eta}^{b-\eta} \right| = \left| \int_{a+\eta}^{b-\eta} \cos 2\pi\varkappa x\,dx \right| \leqq \frac{1}{\pi\varkappa};$$

$$\int_a^{a+\eta} = \int_a^{a+\eta} \frac{x-a}{\eta} \cos 2\pi\varkappa x\,dx = \frac{1}{2\pi\varkappa} \sin 2\pi\varkappa(a+\eta) - \frac{1}{2\pi\varkappa\eta} \int_a^{a+\eta} \sin 2\pi\varkappa x\,dx,$$

also

$$\left|\int_a^{a+\eta}\right| \leqq \frac{1}{2\pi\varkappa} + \frac{\eta}{2\pi\varkappa\eta} = \frac{1}{\pi\varkappa}; \text{ und ebenso } \left|\int_{b+\eta}^{b}\right| \leqq \frac{1}{\pi\varkappa}.$$

Daher ist für $\varkappa = 1, 2, \ldots$

$$|a_\varkappa| < \frac{2}{\varkappa}, \quad \text{und ebenso} \quad |b_\varkappa| < \frac{2}{\varkappa}. \tag{27}$$

Die gleichen Abschätzungen ergeben sich für die Fourierkoeffizienten von $f_2(x)$.

Werden die Teilsummen der Fourierentwickelung von $f_1(x)$ mit $s_\varkappa$ bezeichnet, so konvergiert, da $f_1(x)$ stetig ist, $\frac{1}{p+1}(s_1 + \ldots + s_{p+1})$ gleichmäßig für alle x gegen $f_1(x)$, und zwar ist [6]) der

$$|\text{Fehler}| < \sigma \quad \text{für} \quad p+1 > \frac{3M}{\sigma \sin^2 \delta};$$

dabei bedeutet M das Maximum von $|f_1(x)|$, also hier $M = 1$; ferner ist δ eine solche Zahl, daß

$$|f_1(x-2v) + f_1(x+2v) - 2f_1(x)| < \sigma \quad \text{für} \quad 0 \leqq v \leqq \delta$$

ist. Da

$$|f_1(x-2v) + f_1(x+2v) - 2f_1(x)|$$
$$\leqq |f_1(x+2v) - f_1(x)| + |f_1(x) - f_1(x-2v)| \leqq \frac{2v}{\eta} + \frac{2v}{\eta} = \frac{4v}{\eta}$$

ist, kann hier $\delta = \frac{1}{5}\eta\sigma$ gesetzt werden. Wir haben dann

$$|\text{Fehler}| < \sigma \quad \text{für} \quad p+1 > \frac{3}{\sigma \sin^2 \frac{1}{5}\eta\sigma}.$$

Wird nun $\sigma = n^{\gamma-1}$ gewählt, so folgt hieraus wegen (24)

$$|\text{Fehler}| < n^{\gamma-1} \quad \text{für} \quad p = (10n)^5. \tag{28}$$

Eine gleiche Abschätzung gilt für die arithmetischen Mittel der Fourierentwicklung von $f_2(x)$.

Wird nun für das in (28) festgelegte p

$$\frac{1}{p+1}(s_1 + \ldots + s_{p+1}) = \varphi_1(x) \tag{29}$$

gesetzt und das entsprechende arithmetische Mittel für $f_2(x)$ mit $\varphi_2(x)$ bezeichnet, so folgt aus (26) und (28)

$$\Im > \sum_{h=1}^{n} \left\{\varphi_1(\alpha_h) - \int_0^1 f_1(x)\,dx\right\} - 2n^\gamma,$$

$$\Im < \sum_{h=1}^{n} \left\{\varphi_2(\alpha_h) - \int_0^1 f_2(x)\,dx\right\} + 2n^\gamma.$$

[6]) Z. B. vgl. G. Kowalewski, *Grundzüge der Differential- und Integralrechnung*, Leipzig u. Berlin 1909, S. 284–285.

Das konstante Glied in der trigonometrischen Summe $\varphi_1(x)$ stimmt mit dem konstanten Glied der Fourierentwicklung von $f_1(x)$ überein und ist daher gerade $\int_0^1 f_1(x)\,dx$; entsprechendes gilt für $\varphi_2(x)$. Mithin ist, wenn mit $\psi_1(x)$ bzw. $\psi_2(x)$ die durch Fortlassung des konstanten Gliedes aus $\varphi_1(x)$ bzw. $\varphi_2(x)$ entstehende Funktion bezeichnet wird,

$$|\mathfrak{J}| < \left|\sum_{h=1}^{n} \psi_1(\alpha_h)\right| + \left|\sum_{h=1}^{n} \psi_2(\alpha_h)\right| + 2n^{\nu}. \tag{30}$$

Dabei ist wegen (29) und (27)

$$\begin{aligned}\left|\sum_{h=1}^{n} \psi_1(\alpha_h)\right| &= \left|\sum_{h=1}^{n}\sum_{\varkappa=1}^{p} \frac{p-\varkappa+1}{p+1}\,(a_\varkappa \cos 2\pi\varkappa\alpha_h + b_\varkappa \sin 2\pi\varkappa\alpha_h)\right| \\ &\leqq \sum_{\varkappa=1}^{p} |a_\varkappa| \left|\sum_{h=1}^{n} \cos 2\pi\varkappa\alpha_h\right| + \sum_{\varkappa=1}^{p} |b_\varkappa| \left|\sum_{h=1}^{n} \sin 2\pi\varkappa\alpha_h\right| \\ &\leqq 4 \sum_{\varkappa=1}^{p} \frac{1}{\varkappa} \left|\sum_{h=1}^{n} e(\varkappa\alpha_h)\right|.\end{aligned}$$

Da sich eine gleiche Abschätzung für $\sum \psi_2(\alpha_h)$ ergibt, ist mit (30) wegen (25) die Behauptung bewiesen.

Aus dem eben bewiesenen Satz lassen sich unter Benutzung der Abschätzungen der §§ 1 und 2 die beiden folgenden Sätze ableiten.

Satz 4. *Es sei $k \geqq 2$ und bei gegebenem q, $P_k(u)$*

$$\delta = (q, a_k, a_{k-1}, \ldots, a_1),$$

und es sei $\mathfrak{a}$ ein Intervall mit

$$q^{1-L(k)} \leqq |\mathfrak{a}| \leqq q - q^{1-L(k)}. \tag{31}$$

Dann gibt es zu jedem $\varepsilon > 0$ eine Zahl $C_1 = C_1(\varepsilon)$, so daß

$$q_{\mathfrak{a}} - |\mathfrak{a}| < C_1 k\, \delta^{L(k)}\, q^{1-L(k)+\varepsilon} \tag{32}$$

ist.

Anmerkungen. 1. Die Abschätzung der Herren Hardy und Littlewood für S (vgl. Einleitung) würde auf Grund des Satzes 3 ein ähnliches Resultat ergeben; jedoch würde an Stelle von $C_1\, k\, \delta^{L(k)}$ eine Konstante stehen, die außer von k noch von (q, a_k) abhinge, während hier z. B. für alle Polynome $P_k(u)$ mit $(a_k, \ldots, a_1) = 1$ sich *dieselbe* Abschätzung

$$|q_{\mathfrak{a}} - |\mathfrak{a}|| < C_1 k q^{1-L(k)+\varepsilon}$$

ergibt.

2. Aus dem Satz folgt insbesondere, daß bei gegebenem c die Anzahl der Lösungen der Kongruenz

$$P(u) \equiv c \pmod q$$

bei passend gewähltem $D = D(k, \varepsilon)$ höchstens

$$D\,\delta^{L(k)} q^{1-L(k)+\varepsilon}$$

ist; denn man wähle für $\mathfrak{a}$ ein Intervall der Länge $q^{1-L(k)}$, das c im Innern enthält.

3. Wenn (31) nicht erfüllt ist, ist die Behauptung, wie leicht einzusehen, zwar auch richtig, wird aber dadurch beeinträchtigt, daß das Fehlerglied das Hauptglied überwiegt.

Beweis. Wir wenden Satz 3 an auf $n = q$, $\gamma = 1 - L(k)$, $\alpha_\tau = \frac{1}{q} P(\tau - 1)$ und verstehen unter $\mathfrak{i}$ das Intervall, das durch Verkleinerung der Zahlengeraden im Maßstabe $1 : q$ aus $\mathfrak{a}$ entsteht. Dann ist wegen (31) die Bedingung (22) erfüllt, $J(n) = q_{\mathfrak{a}}$, $n\,|\,\mathfrak{i}\,| = |\,\mathfrak{a}\,|$, und (23) lautet

$$\left| q_{\mathfrak{a}} - |\,\mathfrak{a}\,| \right| < 8 \sum_{\varkappa=1}^{p} \frac{1}{\varkappa} \left| \sum_{u=0}^{q-1} e_q(\varkappa P(u)) \right| + 2 q^{1-L(k)}.$$

Nach (5) folgt hieraus

$$\left| q_{\mathfrak{a}} - |\,\mathfrak{a}\,| \right| < 10\, k\, \delta^{L(k)} q^{1-L(k)} T(q) \sum_{\varkappa}', \tag{33}$$

wo

$$\sum_{\varkappa}' = \sum_{\varkappa=1}^{p} \frac{(q, \varkappa)}{\varkappa} \leqq \sum_{d \mid q} \sum_{\lambda=1}^{p} \frac{d}{\lambda d} \leqq \sum_{d \mid q} (1 + \log p) = T(q)(1 + \log p)$$

ist. Da $p = (10q)^5$ ist, gibt es zu jedem $\varepsilon > 0$ ein $C_1 = C_1(\varepsilon)$, so daß

$$10\, T^2(q)(1 + \log p) < C_1 q^{\varepsilon}$$

ist. Dann ist aber mit (33) die Behauptung (32) bewiesen.

Satz 5. *Es mögen $P(u, v)$ und δ die in Satz 2 und Anmerkung angegebene Bedeutung haben, und es sei $\mathfrak{a}$ ein Intervall, das* (31) *erfüllt; ferner sei $Q_{\mathfrak{a}}$ die Anzahl der* mod q *für $u = 0, 1, \ldots, q-1$ und $v = 0, 1, \ldots, q-1$ in $\mathfrak{a}$ hineinfallenden Polynomwerte $P(u, v)$. Dann gibt es zu jedem $\varepsilon > 0$ eine Zahl $C_2 = C_2(\varepsilon)$, so daß*

$$\left| Q_{\mathfrak{a}} - q\,|\,\mathfrak{a}\,| \right| < C_2 (k!)^2\, \delta^{L(k)} q^{2-L(k)+\varepsilon}.$$

Beweis. Wir wenden Satz 3 an auf $n = q^2$, $\gamma = 1 - \frac{1}{2} L(k)$, $q\alpha_1 = P(0,0), \ldots, q\alpha_q = P(q-1, 0)$; $q\alpha_{q+1} = P(0,1), \ldots, q\alpha_{2q} = P(q-1, 1)$; $q\alpha_{2q+1} = P(0,2), \ldots, q\alpha_{q^2} = P(q-1, q-1)$. Wir verstehen weiter unter $\mathfrak{i}$

wieder das Intervall, das aus $\mathfrak{a}$ durch Verkürzung auf $1:q$ hervorgeht. Dann ist wieder (22) erfüllt, und (23) lautet wegen (10)

$$|Q_{\mathfrak{a}} - q|\mathfrak{a}|| < 8\sum_{\varkappa=1}^{p}\frac{1}{\varkappa}\left|\sum_{u=0}^{q-1}\sum_{v=1}^{q-1} e_q(\varkappa P(u,v))\right| + 2q^{2-L(k)}$$

$$< 10\,(k!)^2\,\delta^{L(k)}\,q^{2-L(k)}\,T(q)\sum_{\varkappa=1}^{p}\frac{(q,\varkappa)}{\varkappa},$$

woraus, wie vorhin, die Behauptung folgt.

§ 4.

Über die Lösungszahl von Kongruenzen k-ten Grades.

Satz 6. *Es sei für das Polynom* $P_k(u)$

$$\delta = (q, a_k, \ldots, a_1).$$

Dann gilt für die Anzahl L_k *der inkongruenten Lösungen der Kongruenz*

$$P_k(u) \equiv 0 \pmod q \tag{34}$$

die Abschätzung

$$L_k \leqq \delta^{1/k}\,T^{k-1}(q)\,q^{1-1/k}. \tag{35}$$

Anmerkungen. 1. Wegen $T(q) = O(q^{\varepsilon})$ ist dieses bezüglich der Größenordnung von q eine erhebliche Verschärfung des in Anm. 2 zu Satz 4 gewonnenen Ergebnisses.

2. Die Kongruenz

$$x^k \equiv 0 \pmod{2^{k\alpha}},$$

die offenbar für jede natürliche Zahl α genau $2^{k\alpha-\alpha} = q^{1-1/k}$ Lösungen hat, zeigt, daß bei jedem k in unendlich vielen Fällen $L_k \geqq q^{1-1/k}$, also bei der für L_k angegebenen Abschätzung der Exponent von q für *beliebige* q keiner beträchtlichen Verkleinerung fähig ist.

3. Die Abschätzung (35) läßt sich weder aus einem kürzlich von Herrn Nagel[7]) angegebenen Ergebnis, noch dieses aus obiger Abschätzung (35) folgern.

Beweis. Für $k = 1$ hat die Kongruenz

$$a_1 u + a_0 \equiv 0 \pmod q$$

höchstens $(a_1, q) = \delta$ Lösungen; d. h. die Behauptung ist richtig.

Die Behauptung sei nunmehr richtig für $k-1$; wir zeigen dann ihre Gültigkeit für k. Wir können annehmen, daß (34) mindestens eine Lösung hat. Dann ist für jede Lösung u ($\equiv$ oder $\not\equiv v$) von (34)

$$a_k u^k + \ldots + a_1 u \equiv a_k v^k + \ldots + a_1 v \pmod q,$$

[7]) *Généralisation d'un théorème de Tchebycheff*, Journal de Mathématiques pures et appliquées (8) **4** (1921), S. 343—356, vgl. S. 345 ff.

also

$$(36)\quad (u-v)\{a_k \sum_{\lambda=0}^{k-1} u^\lambda v^{k-\lambda-1} + a_{k-1} \sum_{\lambda=0}^{k-2} u^\lambda v^{k-\lambda-2} + \ldots + a_1\} \equiv 0 \pmod q.$$

Es werde

$$(u-v, q) = r, \qquad q/r = s$$

gesetzt, so daß $u = v + wr$ ist. Dann folgt aus (36) wegen $(w, s) = 1$

$$(37)\quad \begin{aligned} &a_k \sum_{\lambda=0}^{k-1} \sum_{\mu=0}^{\lambda} w^\mu r^\mu \binom{\lambda}{\mu} v^{k-\mu-1} \\ &+ a_{k-1} \sum_{\lambda=0}^{k-2} \sum_{\mu=0}^{\lambda} w^\mu r^\mu \binom{\lambda}{\mu} v^{k-\mu-2} + \ldots + a_1 \equiv 0 \pmod s. \end{aligned}$$

Bezeichnet $L_{k-1}(s)$ die Anzahl der mod s inkongruenten Lösungen w dieser Kongruenz, so ist offenbar

$$(38)\quad L_k \leqq \sum_{s \mid q} L_{k-1}(s).$$

Um nun die Lösungszahl von (37) abzuschätzen, bemerken wir, daß (37) nur dann Lösungen haben kann, wenn

$$(39)\quad (s, a_k, \ldots, a_2) \mid a_1$$

ist, daß wir also dem s in (38) diese weitere Einschränkung auferlegen können. (37) läßt sich in der Form schreiben

$$w^{k-1} r^{k-1} a_k + w^{k-2} r^{k-2} \sum_{\nu=0}^{1} a_{k-\nu} v^{1-\nu} \sum_{\lambda=k-2}^{k-1-\nu} \binom{\lambda}{k-2}$$

$$v^{k-3} r^{k-3} \sum_{\nu=0}^{2} a_{k-\nu} v^{2-\nu} \sum_{\lambda=k-3}^{k-1-\nu} \binom{\lambda}{k-3} + \ldots + \sum_{\nu=0}^{k-1} a_{k-\nu} v^{k-1-\nu} \sum_{\lambda=0}^{k-1-\nu} \binom{\lambda}{0} \equiv 0 \pmod s.$$

Nach der für $k-1$ als richtig angenommenen Abschätzung (35) ist daher

$$(40)\quad L_{k-1}(s) \leqq T^{k-2}(q)\, s^{1-1/(k-1)}\, \delta_s^{1/(k-1)},$$

wobei

$$\delta_s = \Big(s, r^{k-1} a_k, r^{k-2} \sum_{\nu=0}^{1} a_{k-\nu} v^{1-\nu} \sum_{\lambda=k-2}^{k-1-\nu} \binom{\lambda}{k-2}, r^{k-3} \sum_{\nu=0}^{2} a_{k-\nu} v^{2-\nu} \sum_{\lambda=k-3}^{k-1-\nu} \binom{\lambda}{k-3},$$

$$\ldots, r \sum_{\nu=0}^{k-2} a_{k-\nu} v^{k-2-\nu} \sum_{\lambda=1}^{k-1-\nu} \binom{\lambda}{1}\Big)$$

ist. Hierin vergrößern wir höchstens den Wert der Klammer, indem wir alle Potenzen von r durch r^{k-1} ersetzen. Dann kann aber in jeder $\sum_\nu$

das Glied mit $\nu = 0$ fortgelassen werden, da es ein Vielfaches von $r^{k-1}a_k$ ist, und wir haben

$$\delta_s \leqq \left(s,\ r^{k-1}a_k,\ r^{k-1}a_{k-1},\ r^{k-1}\sum_{\nu=1}^{2},\ r^{k-1}\sum_{\nu=1}^{3},\ \ldots,\ r^{k-1}\sum_{\nu=1}^{k-2}\right)$$

Hier kann in jeder $\sum_\nu$ das Glied mit $\nu = 1$ fortgelassen werden, da es ein Vielfaches von $r^{k-1}a_{k-1}$ ist. Die Fortsetzung dieses Verfahrens führt schließlich zu

$$\delta_s \leqq (s,\ r^{k-1}a_k,\ r^{k-1}a_{k-1},\ \ldots,\ r^{k-1}a_2).$$

Wegen (39) ist dieses

$$\delta_s \leqq (s,\ \delta r^{k-1}) \leqq \operatorname{Min}\{s;\ \delta r^{k-1}\}.$$

Daher ist nach (38) und (40)

$$L_k \leqq T^{k-2}(q) \sum_{s \mid q} \operatorname{Min}\{s;\ \delta^{1/(k-1)} r\, s^{(k-2)/(k-1)}\}$$

$$= T^{k-2}(q) \sum_{s \mid q} \operatorname{Min}\{s;\ u\},$$

wobei wegen $q = rs$ stets u durch $us^{1/(k-1)} = q\,\delta^{1/(k-1)}$ bestimmt ist. Da unter dieser Bedingung $\operatorname{Min}\{s;\ u\}$ am größten für $u = s$ wird, also stets $\leqq \delta^{1/k} q^{1-1/k}$ ist, ergibt sich

$$L_k \leqq T^{k-2}(q) \sum_{s \mid q} \delta^{1/k} q^{1-1/k} = T^{k-1}(q)\,\delta^{1/k} q^{1-1/k};$$

w. z. b. w.

§ 5.

Bedeutung der Abschätzung (6) für das Waringsche Problem.

Es sei t der größte gemeinsame Teiler der Zahlen $P(u) - a_0$ für $u = 1, 2, \ldots$. Herr Landau [8]) hat kürzlich mit der Hardy-Littlewoodschen Methode folgenden Satz bewiesen, der die früher von mir [9]) nach der Hilbertschen Methode gegebene Lösung des allgemeinen Waringschen Problems enthält:

Es gibt ein $s = s(k, a_k)$, so daß für jede durch t teilbare natürliche Zahl $n \geqq n_1(P)$ die diophantische Gleichung

$$n = \sum_{\nu=1}^{s} P(u_\nu), \qquad P(u_\nu) > 0$$

lösbar ist.

[8]) *Zum Waringschen Problem*, Math. Zeitschr. **12** (1922), S. 219—247; Satz V.

[9]) *Verallgemeinerungen des Waring-Hilbertschen Satzes*, Math. Ann. **83** (1921) S. 85—112; Göttinger Inaug.-Diss.

Auf Herrn Landaus Mitteilung hiervon konnte ich mit der Hilbertschen Methode zeigen[10]), daß in vorstehendem Satz bei[11]) $a_0 = 0$ *sogar* s *unabhängig von* a_k gewählt werden kann. Dieses Ergebnis läßt sich auf Grund des § 1 nunmehr auch nach der Hardy-Littlewoodschen Methode gewinnen. Offenbar kann dabei unbeschadet der Allgemeinheit $(a_k, \ldots, a_1) = 1$ angenommen werden. Ferner kann angenommen werden, daß alle Koeffizienten von $P(u)$ positiv sind[12]), so daß die bei Herrn Landau vorkommende Voraussetzung, daß $P(u)$ für $u \geqq 0$ beständig wächst und $\geqq 0$ ist, erfüllt ist. Eine Durchsicht des Beweises von Herrn Landau zeigt, daß es nur darauf ankommt, anstatt des dortigen Hilfssatzes 7 den folgenden, nur wenig abweichenden zu beweisen:

Es seien $a_k, \ldots, a_1$ *sämtlich* > 0, $a_0 = 0$, $(a_k, \ldots, a_1) = 1$, $K = 2^{k-1}$ *und für jede primitive* q*-te Einheitswurzel* ϱ

$$S_\varrho = \sum_{u=1}^{q} \varrho^{P(u)}.$$

1. *Dann ist die Reihe*[13])

$$\mathfrak{S} = \sum_{q=1}^{\infty} \sum_{\varrho} \left(\frac{S_\varrho}{q}\right)^s \varrho^{-n},$$

wo die innere Summe bei jedem q *über alle primitiven* q*-ten Einheitswurzeln zu erstrecken ist, für* $s > 2K$ *und jede natürliche Zahl* n *absolut konvergent.*

2. *Ferner gibt es zu jedem* $\delta > 0$ *ein* $s^* = s^*(k, \delta) > 2K$, *so daß für* $s \geqq s^*$, *für alle durch* t *teilbaren natürlichen Zahlen* n *und für*

$$M = \sum_{q \mid t} \varphi(q)$$

die Ungleichung besteht:

$$M - \delta < \mathfrak{S} < M + \delta.$$

Beweis. 1. Nach (6) ist, da $\varrho = e_q(p)$ mit $(p, q) = 1$ ist,

$$(41) \qquad \sum_{\varrho} \left| \left(\frac{S_\varrho}{q}\right)^s \varrho^{-n} \right| = \sum_{\substack{0 \leqq p < q \\ (p,q)=1}} \left| \frac{1}{q} \sum_{u=1}^{q} e_q(p P(u)) \right|^s < q B^s q^{-s/K + s\varepsilon},$$

wo $B = B(k, \varepsilon)$ nicht von P abhängt. Hieraus folgt aber für jedes $s > 2K$ bei passend gewähltem ε die Behauptung 1.

---

[10]) *Bemerkung zum allgemeinen Waringschen Problem*, Math. Zeitschr. **15** (1922), S. 188–194.

[11]) Diese Bedingung ist *notwendig*; vgl. die in Fußnote [10]) zitierte Arbeit, Anm. 3.

[12]) Vgl. die in Fußnote [10]) zitierte Arbeit; Beweis des Satzes, Vorbemerkung c.

[13]) Die bei Herrn Landau stehende $\sum_{\varrho}$ hat die gleiche Bedeutung wie hier $\sum_{q} \sum_{\varrho}$. Es handelt sich also auch hier um absolute Konvergenz in gleichem Sinne wie dort.

2. Es werde $\varepsilon = \frac{1}{4K}$ gewählt. Dann hängt B höchstens von k ab. Es werde

$$\nu = \nu(k) = [B^{4K}] + 1 \tag{42}$$

gesetzt. Dann ist für $s > 4K$

$$\mathfrak{S} = \sum_{q=\nu+1}^{\infty} + \sum_{\substack{1 \leqq q \leqq \nu \\ q \mid t}} + \sum_{\substack{1 \leqq q \leqq \nu \\ q \nmid t}} = \Sigma_1 + \Sigma_2 + \Sigma_3 . \tag{43}$$

In Σ_1 ist wegen (42)

$$B < \nu^{1/4K} < q^{\frac{1}{4K}}, \tag{44}$$

also wegen (41)

$$|\Sigma_1| \leqq \sum_{q=\nu+1}^{\infty} \sum_{\varrho} \left|\frac{S_\varrho}{q}\right|^s < \sum_{q=\nu+1}^{\infty} q^{1-s/2K},$$

also für $s = \sigma_1(k, \delta) > 2K$

$$|\Sigma_1| < \frac{\delta}{2} . \tag{45}$$

Σ_2 enthält, da wegen (41) und (44) für $q > \nu$

$$\left|\frac{S_\varrho}{q}\right| < q^{-\frac{1}{2K}} < 1$$

ist, also in Σ_1 kein $q \mid t$ enthalten ist, *alle* $q \mid t$, und es ist offenbar für $t \mid n$

$$\Sigma_2 = \sum_{q \mid t} \varphi(q) = M. \tag{46}$$

In Σ_3 ist jedes S_ϱ eine Summe von nicht sämtlich gleichen Einheitswurzeln, da diese sonst sämtlich gleich $\varrho^{P(q)} = 1$ wären, also $q \mid t$ wäre. Daher, und weil $q \leqq \nu(k)$ in Σ_3 ist, gibt es ein $D(k) < 1$, so daß

$$\left|\frac{S_\varrho}{q}\right| < D < 1$$

ist. Mithin ist für $s \geqq \sigma_2(k, \delta)$

$$|\Sigma_3| \leqq \sum_{q=1}^{\nu} \sum_{\varrho} D^s < \frac{\delta}{2} . \tag{47}$$

Da $\mathfrak{S}$ reell ist, ist aber mit (43), (45), (46) und (47) die Behauptung bewiesen.

(Eingegangen am 27. September 1922).

Ein hydrodynamischer Unitätssatz.

Von

Alexander Weinstein in Zürich.

Seit dem Erscheinen der grundlegenden Arbeit von Levi-Civita[1] sind überaus zahlreiche Beispiele von zweidimensionalen, diskontinuierlichen, wirbelfreien Strömungen diskutiert worden[2]. Indessen kennt man bis jetzt keine allgemeine Antwort auf eine prinzipiell wichtige Frage, wie die nach der Existenz oder Eindeutigkeit der Lösung bei vorgegebenen Bedingungen (z. B. festen Grenzen und Geschwindigkeit im Unendlichen).

Ich werde das (zweidimensionale) *Problem des Ausflusses eines freien Strahles* aus einem symmetrischen Gefäß betrachten und zeigen, daß es zu einer gegebenen Strömung keine unendlich benachbarte mit denselben festen Grenzen und demselben Kontraktionskoeffizienten geben kann, vorausgesetzt, daß die Krümmung des gegebenen Strahlrandes eine gewisse (durch die Ungleichung (3) ausgedrückte) Bedingung erfüllt. (Dabei werden nur solche Bewegungen in Betracht gezogen, bei denen außer den Strahlrändern keine weitere freie Grenze auftritt. Strömungsbeispiele, die Thiry[3] und Jaffé[4] gegeben haben, zeigen die Notwendigkeit, diese Hypothese explizite anzuführen.) Die eigentümliche Schwierigkeit des Unitätsbeweises liegt in unserem Fall darin, daß man im Gegensatz zu anderen Problemen der konformen Abbildung nicht mit der Abbildung vorgegebener Bereiche aufeinander zu tun hat.

Ein solcher „*Unitätssatz im Kleinen*“ dient, wie ich zum Schluß noch kurz andeuten werde, bei manchen Problemen als Ausgangspunkt für einen Existenzbeweis nach der Kontinuitätsmethode.

Cisotti[5] hat im Anschluß an die Arbeit von Levi-Civita den analytischen Charakter der möglichen Lösungen des Problems der Strahl-

[1]) Rendiconti del Circolo Matematico di Palermo **23** (1907), S. 1–37.

[2]) Vgl. den zusammenfassenden Bericht von G. Jaffé in der Zeitschrift für angewandte Mathematik und Mechanik **1** (1921), S. 398–410.

[3]) Annales de l'Ecole Normale Supérieure **38** (1921), S. 229–329.

[4]) Physikalische Zeitschrift **23** (1922), S. 129–133.

[5]) Rendiconti del Circolo Matematico di Palermo **25** (1908), S. 145–179.

bildung bestimmt. Wir stellen seine Resultate für den Fall einer *symmetrischen Strömung* zusammen.

Es sei $z = x + iy$ die Stromebene, $\varphi(x, y)$ das Geschwindigkeitspotential; $u = \frac{\partial \varphi}{\partial x}$, $v = \frac{\partial \varphi}{\partial y}$ die Komponenten der Geschwindigkeit. Cisotti trifft eine solche Wahl der Einheiten, daß der absolute Betrag $\sqrt{u^2 + v^2}$ der Geschwindigkeit an den freien Grenzen gleich 1 wird und der Strahl im Unendlichen die Breite π besitzt. Dann wird der (in bezug auf die x-Achse symmetrisch gedachte) Strombereich $A + B$ (Fig. 1) durch eine Funktion $f(z) = \varphi + i\psi$ (ψ bedeutet die zu φ konjugierte Potentialfunktion) umkehrbar eindeutig und im Innern konform auf den in der Fig. 2 gezeichneten Parallelstreifen $S\left(-\infty < \varphi < +\infty,\ -\frac{\pi}{2} \leqq \psi \leqq \frac{\pi}{2}\right)$ von der Breite π in der f-Ebene abgebildet, wobei $\left|\frac{df}{dz}\right| = |w| = |u - iv| \equiv 1$ auf den freien Grenzen ist. Man kann stets erreichen, daß bei dieser Abbildung die festen Wände ω_1, ω_2 des Kanals A und die freien Grenzen λ_1, λ_2 des Strahles B in der durch die Figuren angegebenen Weise den Rändern des Streifens S entsprechen. Aus Symmetriegründen geht die x-Achse in die φ-Achse über.

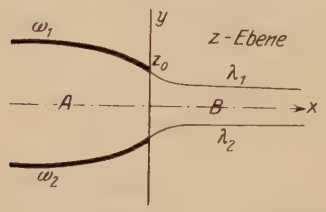


Fig. 1.

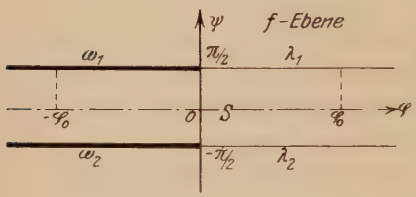


Fig. 2.

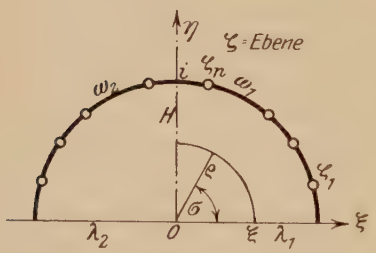


Fig. 3.

An Stelle von f führt Cisotti die Variable $\zeta = \xi + i\eta = \varrho e^{i\sigma}$ ein, indem er den Parallelstreifen konform auf einen Halbkreis H vom Radius 1 um den Nullpunkt der ζ-Ebene (Fig. 3) abbildet. Die Abbildungsformel lautet dann

$$ie^f = \frac{1}{2}\left(\zeta + \frac{1}{\zeta}\right). \tag{1}$$

Es bezeichne ω den mit i multiplizierten Logarithmus von w

$$\omega = i \lg w = \vartheta + i\tau.$$

Wir können ω (und dasselbe gilt von allen in den folgenden Betrachtungen auftretenden Funktionen) entweder als Funktion von ζ, oder von f, oder von z auffassen. Wir werden stets für dieselbe Größe denselben

Buchstaben als Funktionszeichen benutzen, dabei aber, wenn notwendig, die Wahl der unabhängigen Variablen andeuten. $\vartheta(x, y)$ bedeutet den Winkel, den die Richtung der Strömung im Punkte (x, y) mit der x-Achse bildet; τ ist der Logarithmus des Betrages der Geschwindigkeit.

Cisotti zeigt, daß jede (durch die Wahl der Einheiten in der angegebenen Weise normierte) Lösung unseres Problems durch die Formel

$$z = \int_1^{\zeta} e^{i\omega(\zeta)} \frac{\zeta^2 - 1}{\zeta^2 + 1} \frac{d\zeta}{\zeta} + z_0 \tag{2}$$

$\left(\text{d. h. } dz = \frac{df}{w}\right)$, wo ζ die Punkte des Halbkreises H durchläuft, gegeben ist. (Die Lage des Stromgebietes in bezug auf das (x, y)-Achsenkreuz ist aus Fig. 1 ersichtlich; $2|z_0|$ bedeutet die Größe der Öffnung des Kanals.) Für $\omega(\zeta)$ darf man in die Formel (2) eine willkürliche für $|\zeta| < 1$ reguläre Funktion, die reell auf der ξ-Achse ist und für $\zeta = 0$ verschwindet, einsetzen. Es ist $\overline{\omega}(\bar{\zeta}) = \omega(\zeta)$ und es muß (wegen der Symmetrie der Strömung) $\omega(-\zeta) = -\omega(\zeta)$ sein. Wir setzen voraus, daß $\omega(\zeta)$ auch auf der Peripherie des Halbkreises H regulär ist, außer in höchstens endlich vielen Ausnahmepunkten $\zeta_1, \zeta_2, \ldots, \zeta_{2n}$ $(\zeta_h = e^{i\sigma_h};\ 0 < \sigma_1 < \sigma_2 < \ldots < \sigma_n < \frac{\pi}{2};$ $\sigma_{2n-h+1} = \pi - \sigma_h$ für $h = 1, 2, \ldots, n)$. In der Umgebung von ζ_h soll ω sich in der Form

$$\omega(\zeta) = i\beta_h \lg(\zeta - \zeta_h) + \mathfrak{P}(\zeta - \zeta_h),$$

wo $0 < \beta_h < 1$ und $\mathfrak{P}$ eine Potenzreihe bedeutet, darstellen lassen. Dann bestehen die Grenzen ω_1, ω_2 des Kanals aus endlich vielen analytischen Kurvenstücken, die aneinander stoßen und gegen die Strömung konkave Winkel von der Größe $(1 - \beta_h)\pi$ bilden. Damit ω_1 überall gegen die Strömung konkav bleibt und im Unendlichen eine zur x-Achse parallele Asymptote besitzt, muß $\frac{\partial\vartheta(\varrho, \sigma)}{\partial\sigma} < 0$ für $\varrho = 1$, $0 < \sigma < \pi$ und ϑ für $\zeta = i$ gleich Null sein.

Die Formel (2) ist als das allgemeine Integral des Problems zu bezeichnen. Sie liefert alle in der angegebenen Weise normierten symmetrischen Strömungen. Wir können jetzt den behaupteten Unitätssatz folgendermaßen aussprechen:

Zu einer (normierten) zur x-Achse symmetrischen Lösung des Problems der Strahlbildung existiert keine (ebenfalls normierte, symmetrische) unendlich benachbarte Lösung mit unvariiert bleibenden festen Grenzen und Öffnung des Kanals, vorausgesetzt, daß der Realteil ϑ von ω bei der Darstellung der gegebenen Lösung durch eine Formel (2) der Ungleichung

$$\left|\frac{\partial\vartheta(\xi, \eta)}{\partial\xi}\right| < \frac{2}{\pi} \tag{3}$$

für $\eta = 0$ und $0 \leqq \xi \leqq 1$ genügt.

Die Voraussetzung (3) betrifft die Krümmung c des freien Randes, besagt aber nicht, daß diese beschränkt bleiben muß. In der Tat ist z. B. auf λ_1 [6])

$$(4) \qquad c = \left[\frac{\partial \vartheta(\varphi, \psi)}{\partial \varphi}\right]_{\varphi > 0,\, \psi = \frac{\pi}{2}} = \frac{\xi(\xi^2+1)}{\xi^2-1}\left[\frac{\partial \vartheta(\xi, \eta)}{\partial \xi}\right]_{0 \leqq \xi \leqq 1,\, \eta = 0},$$

also im allgemeinen unendlich beim Austrittspunkt z_0. Wir werden einen wichtigen Fall angeben, wo man das Bestehen unserer Voraussetzung bereits aus der Form der festen Grenzen allein einsehen kann.

Eine benachbarte Strömung mit demselben Kanal A und einem unendlich wenig vom gegebenen Strahl B verschiedenen Strahl B_1 würde durch eine Funktion f_1 von z auf denselben Streifen S der Fig. 2 abgebildet, wobei $\left|\frac{df_1}{dz}\right| = 1$ auf den freien Grenzen von B_1 wäre. Jedem Punkt z im Innern des gegebenen Bereiches $A + B$ entsprechen zwei (unendlich benachbarte) Punkte f und f_1 des Streifen S. Ihre Differenz $f_1 - f$, die wir (im Limes) als die Variation δf von f bezeichnen wollen, ist eine in $A + B$ eindeutige analytische reguläre Funktion. Unser Satz behauptet, daß δf identisch verschwindet. Der Funktion f_1 entspricht in der Darstellung der Strömung durch (2) eine Funktion ω_1, der Variation δf von f die Variation $\delta\omega$ von ω. $\delta\omega$ ist eine für $|\zeta| < 1$ reguläre Funktion mit denselben Symmetrieeigenschaften, wie ω selber. Auf der Peripherie $|\zeta| = 1$ besitzt $\delta\omega$ höchstens endlich viele singuläre Stellen (entsprechend den eventuell vorhandenen „Eckpunkten" ζ_h), in deren Umgebung $\delta\omega$ sich in der Form

$$\delta\omega = \frac{-i\beta_h}{\zeta - \zeta_h} + \mathfrak{P}'(\zeta - \zeta_h)$$

darstellen läßt. Da ferner die Geschwindigkeiten beider Strömungen in den unendlich fernen Punkten $x = +\infty$ und $x = -\infty$ übereinstimmen müssen (für $x = +\infty$ ist das eine Folge der Symmetrie der Lösungen, für $x = -\infty$ ergibt sich sodann die Übereinstimmung durch Betrachtung des Flusses durch den Querschnitt des Kanals im Unendlichen), muß $\delta\omega$ sowohl für $\zeta = 0$ als für $\zeta = i$ (mindestens in der ersten Ordnung) verschwinden.

Es ist leicht, δf durch $\delta\omega$ auszudrücken. Einem inneren Punkt z von $A + B$ entspricht, je nachdem wir ihn als Punkt der gegebenen oder der benachbarten Strömung auffassen, ein Punkt ζ bzw. ζ_1 $(= \zeta + \delta\zeta$ des ζ-Halbkreises. Aus (2) folgt sofort

$$0 = e^{i\omega(\zeta)}\frac{\zeta^2-1}{\zeta^2+1}\frac{\delta\zeta}{\zeta} + i\int_1^{\zeta} e^{i\omega(\zeta)}\,\delta\omega\,\frac{\zeta^2-1}{\zeta^2+1}\frac{d\zeta}{\zeta},$$

[6]) Vgl. loc. cit. [1]), S. 17.

und da nach (1)

$$\delta f = \frac{\zeta^2 - 1}{\zeta^2 + 1} \frac{\delta \zeta}{\zeta}$$

ist, haben wir

$$\delta f = i e^{-i\omega(\zeta)} \int_1^{\zeta} e^{i\omega(\zeta)} \delta\omega \frac{1-\zeta^2}{1+\zeta^2} \frac{d\zeta}{\zeta} .$$

δf ist, im Gegensatz zu f selber, eine beschränkte Funktion, die, wie aus dem über ω und $\delta\omega$ Gesagten folgt, sowohl bei $\zeta = 0$ wie bei $\zeta = i$ regulär bleibt. In den „Eckpunkten" ζ_h ist δf stetig, während $\frac{d(\delta f)}{d\zeta}$ dem absoluten Werte nach wie $\frac{1}{|\zeta - \zeta_h|^{1-\beta_h}}$ unendlich werden kann.

Wir wollen nun die Bedingungen betrachten, denen $\delta f = \delta\varphi + i\delta\psi$ am Rande des gegebenen Strombereiches genügen muß.

Ein Punkt z des Randes ω_1 wird sowohl durch f als durch f_1 auf (benachbarte) Punkte des oberen Randes $\psi = \frac{\pi}{2}$ von S abgebildet. Somit ist

$$\delta\psi = 0 \tag{5}$$

auf ω_1 (und selbstverständlich dann auch auf ω_2). Einen solchen Schluß kann man nicht für einen Punkt z des freien Randes λ_1 machen, da dieses z nicht zugleich Randpunkt des Strahles der benachbarten Lösung zu sein braucht. Wir verfahren deswegen folgendermaßen. Neben dem Punkt z von λ_1, dem bei der Abbildung durch die Funktion f ein bestimmter Punkt $\varphi + \frac{i\pi}{2}$ $(\varphi > 0)$ des Streifens S entspricht, betrachten wir denjenigen Punkt $z + \delta z$ des freien Randes des Strahles B_1, dem die Funktion f_1 genau denselben Punkt $\varphi + \frac{i\pi}{2}$ zuordnet. Dann haben wir

$$f_1(z + \delta z) = f(z)$$

oder, indem wir uns auf Glieder erster Ordnung beschränken,

$$f_1(z) + \delta z \left(\frac{df}{dz}\right)_z = f(z),$$

woraus im Limes folgt

$$\delta f = -\frac{df}{dz} dz \tag{6}$$

für jedes z an der freien Grenze. Um die unbekannte Verschiebung δz aus (6) zu eliminieren, schreiben wir die Gleichung

$$\left(\frac{df_1}{dz}\right)_{z+\delta z} = e^{i\varepsilon} \left(\frac{df}{dz}\right)_z = (1 + i\varepsilon) \left(\frac{df}{dz}\right)_z$$

an, welche besagt, daß $\frac{df_1}{dz}$ an der Stelle $z + \delta z$ und $\frac{df}{dz}$ an der Stelle z

zwei unendlich benachbarte Zahlen, beide vom absoluten Betrage 1, sind. Bis auf Glieder höherer Ordnung ist dann

$$\left(\frac{df_1}{dz}\right)_z + \delta z \left(\frac{d^2 f}{dz^2}\right)_z - \left(\frac{df}{dz}\right)_z = i\varepsilon \left(\frac{df}{dz}\right)_z,$$

woraus, indem wir für δz seinen Wert aus (6) einsetzen, folgt

$$\Re\left\{\left(\frac{d(\delta f)}{dz} - \frac{\delta f}{\frac{df}{dz}}\frac{d^2 f}{dz^2}\right)\frac{1}{\frac{df}{dz}}\right\} = 0$$

für jedes z auf λ_1 und λ_2. ($\Re\{\}$ bedeutet den Realteil von $\{\}$.) Fassen wir nun δf und $\frac{df}{dz} = w$ als Funktionen der unabhängigen Variablen f auf, so erhalten wir hieraus die für $\varphi > 0$, $\psi = \pm\frac{\pi}{2}$ gültige Gleichung

$$\Re\left\{\frac{d(\delta f)}{df} - \frac{d \lg w}{df}\delta f\right\} = 0.$$

Nun ist am freien Rand

$$\lg w = -i\vartheta,$$

somit haben wir den Realteil von

$$\frac{\partial(\delta\varphi)}{\partial\varphi} + i\frac{\partial(\delta\psi)}{\partial\varphi} + i\frac{\partial\vartheta}{\partial\varphi}(\delta\varphi + i\delta\psi)$$

gleich Null zu setzen. ($\delta\varphi$, $\delta\psi$ und ϑ sind hier als Funktionen von φ und ψ aufzufassen.) Wegen $\frac{\partial(\delta\varphi)}{\partial\varphi} = \frac{\partial(\delta\psi)}{\partial\psi}$ ergibt sich als Randbedingung für $0 < \varphi < +\infty$, $\psi = \pm\frac{\pi}{2}$:

$$\frac{\partial(\delta\psi)}{\partial\psi} - \frac{\partial\vartheta}{\partial\varphi}\delta\psi = 0, \tag{7}$$

und (5) liefert

$$\delta\psi = 0 \tag{8}$$

für $-\infty < \varphi \leqq 0$, $\psi = \pm\frac{\pi}{2}$.

In (7) und (8) haben wir Randbedingungen, in welchen der Imaginärteil $\delta\psi$ von δf *allein* vorkommt. Im Falle der Symmetrie kommt noch das Bestehen der Gleichung

$$\delta\psi = 0 \tag{9}$$

für $-\infty < \varphi < +\infty$, $\psi = 0$ hinzu. Im Innern von S ist $\delta\psi$ eine reguläre Potentialfunktion.

Wir haben bei der Ableitung der Gleichung (7) von den Funktionswerten von f_1 in Punkten des Randes λ_1 gesprochen, wo doch λ_1 nicht ganz zum ursprünglichen Definitionsbereich $(A + B_1)$ von f_1 zu gehören

braucht. Der kürzeste Weg, das Bestehen von (7) sicherzustellen, ist die Bemerkung, daß (wie man leicht verifizieren kann) (7) das Verschwinden des Realteils der (auch auf der ξ-Achse regulären) Funktion $\delta\omega(\zeta)$ für $0 \leqq \xi \leqq 1$, $\eta = 0$ zum Ausdruck bringt.

Wir haben das identische Verschwinden von $\delta\psi$ zu zeigen. Aus Symmetriegründen genügt es, $\delta\psi$ in der oberen Hälfte $0 \leqq \psi \leqq \frac{\pi}{2}$ des Parallelstreifens zu betrachten. Dann hat man (9) als Randbedingung für $\psi = 0$. Da ferner am oberen Rande von S $\frac{\partial}{\partial\psi} = -\frac{\partial}{\partial n_i}$ ist (n_i bedeutet die innere Normale in bezug auf S), haben wir auch in (7) eine Randbedingung vom bekannten Typus vor uns.

Wir haben also in üblicher Weise das Verschwinden von $\delta\psi$ aus der Betrachtung des Dirichletschen Integrales

$$D(\delta\psi) = \int_0^{\frac{\pi}{2}} \int_{-\infty}^{+\infty} \left\{ \left[\frac{\partial(\delta\psi)}{\partial\varphi}\right]^2 + \left[\frac{\partial(\delta\psi)}{\partial\psi}\right]^2 \right\} d\varphi\, d\psi \tag{10}$$

mit Hilfe der Greenschen Formel zu erschließen. D ist als uneigentliches Integral aufzufassen. Man kann sich leicht von seiner Existenz überzeugen, indem man an Stelle von φ, ψ die Variablen ξ, η einführt, D nach der Greenschen Formel in ein Randintegral verwandelt und aus dem Integrationsweg (der Berandung des Halbkreises H) die Punkte $\zeta = 0$, $\zeta = i$ sowie die „Eckpunkte" ζ_h durch infinitesimale Halbkreise ausschließt. Der Beitrag, der von diesen Halbkreisen herrührt, ist nach dem über das Verhalten von δf und $\frac{d(\delta f)}{d\zeta}$ Gesagten in der Grenze Null. Die Existenz von D ist eine Folge unserer Einschränkung auf Betrachtung von *symmetrischen* Strömungen allein. Das Integral (10) ergibt sich somit als Limes des Randintegrals R von $-\frac{\partial(\delta\psi)}{\partial n_i}$, erstreckt im positiven Sinne über die Berandung des (unendlich langen) Rechteckes mit den Ecken $(\pm\varphi_0, 0)$, $\left(\pm\varphi_0, \frac{\pi}{2}\right)$ der Fig. 2 für $\varphi_0 = +\infty$, wobei die Integration über die punktierten Querseiten in der Grenze keinen Beitrag liefert. Mit Hilfe der Randbedingungen (7), (8) und (9) erhält man

$$D(\delta\psi) = \int_0^{\infty} \left[\frac{\partial\vartheta}{\partial\varphi}(\delta\psi)^2\right]_{\psi=\frac{\pi}{2}} \delta\varphi\,. \tag{11}$$

Das Verschwinden von $\delta\psi$ würde sich hieraus sofort ergeben, falls $\frac{\partial\vartheta(\varphi,\psi)}{\partial\varphi}$ für $0 \leqq \varphi < +\infty$, $\psi = \frac{\pi}{2}$ durchweg $\leqq 0$ wäre. Nun ist aber

ϑ für $\varphi = 0$, $\psi = \frac{\pi}{2}$, d. h. im Punkte z_0 der Fig. 1 negativ, während es im unendlich fernen Punkte des Strahlrandes $\left(\varphi = +\infty,\ \psi = \frac{\pi}{2}\right)$ verschwindet. $\frac{\partial \vartheta}{\partial \varphi}$ kann also nicht stets $\leqq 0$ sein. Vielmehr wird $\frac{\partial \vartheta}{\partial \varphi}$, wenn man Fälle betrachtet, bei welchen ϑ monoton variiert — und nur solche Strömungen sind als Lösungen des Problems der vena contracta annehmbar —, durchweg *positiv* sein. Dies wird sich auch an den zu besprechenden Beispielen bestätigen. Es ist auch zu beachten, daß $\frac{\partial \vartheta}{\partial \varphi}$ nach (4) bei $\varphi = \frac{\pi}{2}$ (positiv) unendlich wird. Die Dinge liegen also wesentlich anders wie in der Theorie der Wärmeleitung.

Wir wollen nun ohne irgendwelche Annahme über das Vorzeichen von $\frac{\partial \vartheta}{\partial \varphi}$, allein unter der Voraussetzung (3) das Verschwinden von $\delta\psi$ beweisen.

$\frac{\partial \vartheta}{\partial \varphi}$ ist, wie erwähnt, bei $\varphi = 0$, $\psi = \frac{\pi}{2}$ unendlich. Wir verpflanzen deswegen beide Integrale D und R der Gl. (11) auf die ξ, η-Ebene. D bleibt dabei invariant. Dasselbe gilt auch vom Randintegral R, welches sich in

$$R = \int_1^0 \left(\frac{\partial \vartheta}{\partial \xi}\right)_{\eta=0} (\delta\psi)^2_{\eta=0}\, d\xi$$

verwandelt. Wegen (3) ist

$$|R| \leqq \frac{2}{\pi} \int_0^1 (\delta\psi)^2_{\eta=0}\, d\xi, \tag{12}$$

wobei das Gleichheitszeichen *nur* beim identischen Verschwinden von $\delta\psi$ für $0 \leqq \xi \leqq 1$, $\eta = 0$ gilt. Den Wert des Integrals $\int_0^1 (\delta\psi)^2\, d\xi$ können wir aber mit dem Wert von D vergleichen. Es ist nach (9) $\delta\psi = 0$ für $\xi = 0$, $0 \leqq \eta \leqq 1$. Also ist für jedes $0 \leqq \xi \leqq 1$

$$-\delta\psi(\xi, 0) = \int_0^{\frac{\pi}{2}} \left[\frac{\partial(\delta\psi)}{\partial \sigma}\right]_{\varrho=\xi} d\sigma,$$

wobei $\delta\psi$ rechter Hand als Funktion der Polarkoordinaten ϱ, σ aufzufassen ist. Die Anwendung der *Schwarzschen Ungleichung* liefert

$$[\delta\psi(\xi, 0)]^2 \leqq \frac{\pi}{2} \int_0^{\frac{\pi}{2}} \left[\frac{\partial(\delta\psi)}{\partial \sigma}\right]^2_{\varrho=\xi} d\sigma.$$

Also ist

$$\int_0^1 (\delta\psi)_{\eta=0}^2 \, d\xi \leqq \frac{\pi}{2} \int_0^1 \int_0^{\frac{\pi}{2}} \left[\frac{\partial(\delta\psi)}{\partial\sigma}\right]^2 d\sigma \, d\varrho,$$

und das ist wegen $\varrho \leqq 1$

$$\leqq \frac{\pi}{2} \int_0^1 \int_0^{\frac{\pi}{2}} \left\{ \left[\frac{\partial(\delta\psi)}{\partial\sigma}\right]^2 \frac{1}{\varrho} + \left[\frac{\partial(\delta\psi)}{\partial\varrho}\right]^2 \varrho \right\} d\sigma \, d\varrho = \frac{\pi}{2} D(\delta\psi).$$

In Verbindung mit (12) folgt daraus, daß das Integral R

$$\int_0^{\infty} \left(\frac{\partial\vartheta}{\partial\varphi}\right)_{\psi=\frac{\pi}{2}} (\delta\psi)^2 \, d\varphi$$

stets *kleiner* als $D(\delta\psi)$ (im Widerspruch mit (11)) wäre, sofern $\delta\psi$ nicht identisch für $0 \leqq \xi \leqq 1$, $\eta = 0$ verschwindet. Das Bestehen von (11) zieht somit dieses Verschwinden von $\delta\psi$ nach sich, somit (immer wegen (11)) das Verschwinden von $\delta\psi$ überhaupt. Da nun δf z. B. für $\varphi = 0$, $\psi = \frac{\pi}{2}$ gleich Null ist, haben wir die Behauptung des Unitätssatzes:

$$\delta f \equiv 0$$

bewiesen.

Wir betrachten nun einige *Beispiele* von Strömungen, für welche die Voraussetzungen für die Gültigkeit unseres Unitätssatzes erfüllt sind.

1. Setzt man $\omega(\zeta) = \vartheta_1 \zeta$, wo $-\frac{2}{\pi} < \vartheta_1 < 0$ ist, so erhält man eine Strahlbildung beim Ausfluß aus einem krummlinig begrenzten symmetrischen Gefäß, wobei ϑ_1 den Winkel zwischen der Richtung der Strömung in der $+x$-Achse im Punkte z_0 bedeutet. Die Breite Ω_1 des Strahles im Unendlichen ist πe^{ϑ_1}, der Kontraktionskoeffizient α ist $< \frac{1}{2 - e^{\vartheta_1}}$. Die Krümmung der festen Wände erreicht für $z = z_0$ ihren größten Wert $c_{\max} = -\vartheta_1 e^{\vartheta_1}$.

2. Besonders interessant ist der Fall einer polygonalen Begrenzung. Setzt man mit Cisotti[7])

$$(13) \qquad \omega(\zeta) = \frac{i}{\pi} \sum_{h=1}^{2n} (\vartheta_{h+1} - \vartheta_h) \log i \frac{\zeta - \zeta_h}{1 - \zeta\zeta_h}$$

in Gl. (2) ein, wobei $\vartheta_1 < \vartheta_2 < \ldots < \vartheta_n < 0$, $\vartheta_{2n+2-h} = -\vartheta_h$ für $h = 1, 2, \ldots, n$, $\frac{\vartheta_{h+1} - \vartheta_h}{\pi} = \beta_h < 1$, $\zeta_h = e^{i\sigma_h} = \xi_h + i\eta_h$, $0 < \sigma_1 < \sigma_2 < \ldots < \sigma_n < \frac{\pi}{2}$ und

[7]) Vgl. loc. cit. [5]) S. 169.

$\sigma_{2n-h+1} = \pi - \sigma_h$ für $h = 1, 2, \ldots, n$ ist, so erhält man eine Strömung mit symmetrischem *polygonalem* festen Rand, der gegen die Strömung konkave Innenwinkel von der Größe $(1-\beta_h)\pi$ besitzt.

Es ist für $0 \leqq \xi \leqq 1$, $\eta = 0$

$$\frac{\partial \vartheta(\xi,\eta)}{\partial \xi} = -\sum_{h=1}^{2n} \beta_h \frac{\sin \sigma_h}{|\xi - \zeta_h|^2} = -\sum_{h=1}^{2n} \beta_h \frac{\eta_h}{(\xi-\xi_h)^2+\eta_h^2},$$

oder indem wir die Beiträge je zweier in bezug auf die η-Achse symmetrischen Punkte ζ_h zusammenfassen:

$$\frac{\partial \vartheta}{\partial \xi} = -\sum_{h=1}^{n} \beta_h \left[\frac{\eta_h}{(\xi-\xi_h)^2+\eta_h^2} + \frac{\eta_h}{(\xi+\xi_h)^2+\eta_h^2}\right].$$

Somit ist (immer für $0 \leqq \xi \leqq 1$, $\eta = 0$)

$$\left|\frac{\partial \vartheta}{\partial \xi}\right| < \sum_{h=1}^{n} \beta_h \left[\frac{1}{\eta_h} + \eta_h\right] < \left(\frac{1}{\eta_1} + \eta_1\right) \sum_{h=1}^{n} \beta_h = -\left(\frac{1}{\eta_1} + \eta_1\right) \frac{\vartheta_1}{\pi}.$$

Der Unitätssatz ist gültig, sofern

$$-\vartheta_1 \left(\eta_1 + \frac{1}{\eta_1}\right) \leqq 2 \tag{14}$$

ist. Gibt man die Neigung ϑ_1 der ersten Wand $z_0 z_1$ des Kanals (die dem Bogen $(1, \zeta_1)$ entspricht) — man könnte sagen: die Totalkrümmung ϑ_1 der festen Grenze — vor, so darf η_1 $(0 < \eta_1 < 1)$ nicht unter einer aus (14) zu bestimmenden Schranke η_0 $(0 < \eta_0 < 1)$ heruntersinken. Diese Schranke η_0 existiert, sofern $|\vartheta_1|$ nicht zu groß, nämlich < 1 ist. Die Ungleichung $\eta_1 \geqq \eta_0$ besagt dann, daß die Länge l_1 der ersten Seite $z_0 z_1$, wie man sich leicht überzeugt, sicher der Bedingung

$$l_1 > \int_0^{\eta_0} \left(\frac{\eta_0+\eta}{\eta_0-\eta}\right)^{-\frac{\vartheta_1}{\pi}} \frac{\eta\, d\eta}{1-\eta^2}$$

genügt. Dann ist der Unitätssatz für die Lösung (13) gültig. Setzt man z. B. $\vartheta = -\frac{\pi}{4}$, so kann man für η_0 z. B. den Wert $\frac{1}{2}$ nehmen und l_1 ist dann $> \int_0^{\frac{1}{2}} \sqrt[4]{\frac{1+2\eta}{1-2\eta}} \frac{\eta\, d\eta}{1-\eta^2}$.

Wir sehen, daß man dem Unitätssatz in unserem Fall eine Formulierung geben kann, in der Voraussetzungen nur in bezug auf die festen Grenzen vorkommen. Wir können z. B. insbesondere behaupten:

Zwei unendlich benachbarte Funktionen ω vom Typus (13) können nicht dasselbe polygonale Profil von einer Totalkrümmung $\leqq \frac{\pi}{4}$ liefern, wenn die Länge l_1 der ersten Seite den Wert 4 übersteigt.

Setzt man (13) in (2) ein, so bekommt man

$$z = i^{\frac{2\vartheta_1}{\pi}} \int_1^{\zeta} \prod_{h=1}^{2n} \left(\frac{1-\zeta\zeta_h}{\zeta-\zeta_h}\right)^{\beta_h} \frac{\zeta^2-1}{\zeta^2+1} \frac{d\zeta}{\zeta} + z_0. \tag{15}$$

Die Cisottische Formel (15) ist gewissermaßen eine Verallgemeinerung der Schwarzschen Formel für die Abbildung eines geradlinigen Polygons auf einen Kreis. Für dieses letztere Problem kann man aus den obigen Betrachtungen einen elementaren Beweis für die Möglichkeit der Konstantenbestimmung in der Schwarzschen Formel ableiten: Aus dem entsprechenden „Unitätssatz im Kleinen" folgt *das Nichtverschwinden der Funktionaldeterminante* der Ableitungen der Seitenlängen nach den Parametern (die unseren ζ_h entsprechen). Der Beweis wird ergänzt durch eine Betrachtung, die den sogenannten *Limessatz* liefert.

Es ist mir eine angenehme Pflicht, Herrn Professor H. Weyl für seine Anregung, das Problem des freien Strahles nach der Kontinuitätsmethode zu behandeln, meinen aufrichtigsten Dank auszusprechen.

(Eingegangen am 10. Dezember 1922.)

Algebraische Gleichungen mit primitiven Gruppen.

Von

Öystein Ore in Kristiania.

Herr Furtwängler[1]) hat neulich ein einfaches Kriterium für die Primitivität von Gleichungen angegeben, indem er den folgenden Satz bewiesen hat:

Wenn in der irreduziblen Gleichung

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

mit ganzen, rationalen Koeffizienten alle Koeffizienten a_i durch die Primzahl p teilbar sind, a_n durch p^2, a_{n-1} aber nicht durch p^2 teilbar, so ist die Gleichung primitiv.

Es soll in dieser Arbeit gezeigt werden, daß dieser Satz ein einfacher Spezialfall allgemeinerer Sätze ist, und weiter sollen verschiedene andere Sätze aufgestellt werden, die damit in Zusammenhang stehen.

§ 1.

Sei

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \tag{1}$$

ein Polynom, dessen Koeffizienten ganze, algebraische Zahlen in einem Körper $P(\theta)$ sind. Sei weiter $\mathfrak{p}$ ein beliebiges Primideal des Körpers und im allgemeinen

$$[a_i] = \mathfrak{p}^{\alpha_i}\mathfrak{a}_i \qquad (i = 1, 2, \ldots, n)$$

die Primidealzerlegung des Hauptideals a_i, wo α_i so gewählt werden soll, daß $\mathfrak{a}_i$ nicht durch $\mathfrak{p}$ teilbar ist. Wenn a_i nicht durch $\mathfrak{p}$ teilbar ist, wird also $\alpha_i = 0$. Man kann dann die Zahlenpaare

$$(0, 0),\ (1, \alpha_1), \ldots, (n, \alpha_n)$$

[1]) Ph. Furtwängler, Über Kriterien für irreduzible und für primitive Gleichungen, Math. Ann. 85, S. 34.

in ein rechtwinkliges Koordinatensystem einzeichnen und zu diesen Gitterpunkten ein Newtonsches Polygon S zeichnen. Dumas[2]) hat nun für den Bereich der rationalen Zahlen (wenn also $\mathfrak{p} = p$ eine rationale Primzahl ist) den folgenden, wichtigen Satz bewiesen:

Das Polygon eines Produkts ist aus den Seiten der Polygonen der Faktoren in der Weise zusammengesetzt, daß die Seiten nach steigender Neigung geordnet werden.

Es ist jetzt bedeutungsvoll, daß dieser Satz auch für einen beliebigen Körper $P(\theta)$ und ein beliebiges Primideal $\mathfrak{p}$ richtig bleibt, was ziemlich einfach gezeigt werden kann, indem man das Beweisverfahren von Dumas anwendet. Daraus folgt sofort die Richtigkeit des Dumasschen Reduzibilitätssatzes für einen beliebigen Körper.

Es seien

$$S_1, S_2, \ldots, S_r$$

die Seiten des Polygons S, und weiter

$$h_1, h_2, \ldots, h_r, \qquad l_1, l_2, \ldots, l_r$$

die Längen der Projektionen dieser Seiten auf die Y-Achse bzw. die X-Achse. e_i soll der größte gemeinsame Faktor von h_i und l_i sein, also

$$\begin{aligned} h_i &= e_i \varkappa_i \\ l_i &= e_i \lambda_i \end{aligned} \qquad (i = 1, 2, \ldots, r),$$

wo λ_i zu $\varkappa_i$ relativ prim ist. Es gilt dann der Satz:

Soll $f(x)$ in $P(\theta)$ reduzibel sein, so kann $f(x)$ keine andere Faktoren haben als von den Graden

$$m = \sum_{i=1}^{r} \tau_i \lambda_i, \tag{2}$$

wo τ_i eine der Zahlen $0, 1, \ldots, e_i$ ist.

In diesem Satze sind die Sätze von Königsberger[3]) und Perron[4]), sowie die Irreduzibilitätssätze von Furtwängler[5]) enthalten. In einer neulich erschienenen Arbeit[6]) habe ich gezeigt, wie man einen noch allgemeineren Irreduzibilitätssatz aufstellen kann, worin außer dem hier erwähnten Satz auch die Sätze von Schönemann[7]) und Bauer[8]) enthalten sind.

---

[2]) Dumas, Sur quelques cas d'irreductibilité des polynomes etc., Journ. de Math. (6) **2**, S. 217.

[3]) L. Königsberger, Über den Eisensteinschen Satz, Journ. für Math. **115**, S. 69.

[4]) O. Perron, Über eine Anwendung der Idealtheorie usw., Math. Ann. **60**, S. 448.

[5]) Loc. cit.

[6]) Math. Zeitschr. **18** (1923), S. 278.

[7]) Schönemann, Über diejenigen Moduln usw., Journ. für Math. **32**, S. 100.

[8]) M. Bauer, Eine Verallgemeinerung eines Satzes von Schönemann, Journ. für Math. **128**, S. 87.

§ 2.

Es soll jetzt vorausgesetzt werden, daß in (1) alle Koeffizienten ganze, rationale Zahlen sind, außerdem soll die Gleichung irreduzibel, also ihre Gruppe transitiv sein. Weiter soll vorausgesetzt werden, daß diese Gruppe imprimitiv ist und die s Systeme der Imprimitivität aus m Gliedern bestehen, folglich $n = ms$.

Im folgenden soll die Zahl m, die die Anzahl der Ziffern in einem Imprimitivitätssystem angibt, eine *Imprimitivitätszahl* der Gruppe genannt werden. Bekanntlich kann eine gegebene Gruppe mehrere Imprimitivitätszahlen besitzen. Wenn die Gleichung imprimitiv sein soll, gibt es einen algebraischen Körper $P(\theta)$ vom s-ten Grade derart, daß $f(x)$ in $P(\theta)$ reduzibel wird und zwar einen Faktor vom Grade m hat.

Sei jetzt wie früher S ein Polygon für $f(x)$ für die Primzahl p bestimmt und

$$p = \mathfrak{p}_1^{u_1} \mathfrak{p}_2^{u_2} \dots \mathfrak{p}_t^{u_t} \tag{3}$$

die Primidealzerlegung von p in $P(\theta)$. Von den Primidealen $\mathfrak{p}_i$ soll eines hervorgehoben werden, indem

$$p = \mathfrak{p}^u \mathfrak{a}$$

gesetzt wird, wo $\mathfrak{a}$ nicht durch $\mathfrak{p}$ teilbar ist. Es soll nun das Polygon S' von $f(x)$ für das Primideal $\mathfrak{p}$ bestimmt werden, und dies ergibt sich einfach aus dem Polygone S. Die Anzahl der Seiten bleibt unverändert und die Projektion einer Seite S_i' auf die X-Achse wird gleich l_i, während die Projektion auf die Y-Achse gleich $u h_i$ ist. Dann muß nach (2) die Gleichung

$$m = \sum_{i=1}^{r} \tau_i \frac{l_i}{f_i} \tag{4}$$

gültig sein, wo f_i der größte gemeinsame Faktor von l_i und $u h_i$, und τ_i eine der Zahlen $0, 1, \dots, f_i$ ist. Es ist aber

$$l_i = e_i \lambda_i, \qquad u h_i = e_i u \varkappa_i,$$

so daß

$$f_i = e_i g_i$$

wird, wo g_i der größte gemeinsame Faktor von λ_i und u ist. Es sei weiter

$$\lambda_i = g_i \lambda_i', \qquad u = g_i u_i'$$

gesetzt. Man kann dann mit diesen Bezeichnungen die Gleichung (4) in der Form

$$m = \sum_{i=1}^{r} \tau_i \frac{\lambda_i}{g} \tag{5}$$

schreiben, oder auch

$$m = \sum_{i=1}^{r} \tau_i \frac{\lambda_i u_i'}{u},$$

woraus

$$m u = \sum_{i=1}^{r} \tau_i \lambda_i u_i' \tag{6}$$

folgt.

Soll also die Gleichung $f(x) = 0$ imprimitiv werden, so sind nur solche Imprimitivitätszahlen möglich, die eine Gleichung von der Form (4) (oder (6)) befriedigen, wo also m ein Teiler von n, τ_i eine der Zahlen $0, 1, \ldots, f_i$ und $u \leqq \frac{n}{m}$ ist.

Die letzte Bedingung kommt hinzu, weil der Grad von $P(\theta)$ gleich $\frac{n}{m}$ ist.

Durch Anwendung dieses Satzes kann man eine Reihe von einfachen Imprimitivitätssätzen aufstellen. Es soll erstens der Fall behandelt werden, daß die Anzahl der Seiten gleich zwei ist, also in (4) $r = 2$. Die Gleichung (6) liefert dann

$$m u = \tau_1 \lambda_1 u_1' + \tau_2 \lambda_2 u_2'. \tag{7}$$

Weiter soll vorausgesetzt werden, daß die Projektion einer Seite gleich 1 ist, also z. B. $l_1 = \lambda_1 = 1$, wobei es unwesentlich ist, ob diese Seite die erste oder die zweite ist. Dann wird $l_2 = n - 1$, und wenn noch vorausgesetzt wird, daß h_2 zu $n - 1$ relativ prim ist, wird auch

$$l_2 = \lambda_2 = n - 1 \quad \text{und} \quad h_2 = \varkappa_2.$$

Dann liefert die Gleichung (7)

$$u m = \tau_1 u_1' + \tau_2 (n-1) u_2'. \tag{8}$$

Hier ist aber

$$u = u_1' g_1 = u_2' g_2,$$

wo wie früher g_i der größte gemeinsame Faktor von λ_i und u ist. Da aber $\lambda_1 = 1$ ist, wird $u_1' = u$ und die Gleichung (8) geht in

$$u(m - \tau_1) = \tau_2 (n-1) u_2'$$

über, wo τ_1 entweder 0 oder 1 ist. Wenn $\tau_1 = 0$ ist, folgt

$$u m = \tau_2 u_2' (n-1),$$

und da m zu $n-1$ relativ prim ist, kommt

$$u = n - 1,$$

was aber nicht möglich ist, da man immer $u \leqq \frac{n}{2}$ voraussetzen kann. Daher ist $\tau_1 = 1$, also

$$u(m-1) = \tau_2 u_2' (n-1).$$

Sei jetzt e der größte gemeinsame Faktor von $n-1$ und $m-1$. Dann folgt

$$u = k\frac{n-1}{e},$$

wo k eine ganze Zahl ist.

Dies muß für alle Exponenten in (3) gelten, es ist also in $P(\theta)$

$$p = (\mathfrak{p}_1^{k_1}\mathfrak{p}_2^{k_2}\dots\mathfrak{p}_t^{k_t})^{\frac{n-1}{e}},$$

folglich

$$s = (k_1 f_1 + k_2 f_2 + \dots k_t f_t)\frac{n-1}{e},$$

wo f_i der Grad von $\mathfrak{p}_i$ ist. Dies ist aber nicht möglich, denn s ist ein Teiler von n und kann daher nicht durch einen Teiler von $n-1$ teilbar sein. Es ist folglich $e = n-1$, also $m = n$, d. h. die Gleichung ist primitiv. Dadurch ist die Richtigkeit des Satzes bewiesen:

Satz 1. *Sei $f(x) = 0$ eine irreduzible Gleichung mit einem zweiseitigen Polygon, dessen eine Seite eine Projektion auf die X-Achse gleich 1 hat. Wenn für die andere Seite h_2 zu $n-1$ relativ prim ist, wird die Gleichung primitiv.*

Daß der oben angeführte Satz von Furtwängler in diesem Satze enthalten ist, ist offenbar. Man kann aber auch mehrere andere einfache Primitivitätssätze ableiten, die von Interesse sind. So hat man z. B. den folgenden Satz:

Satz 2. *Wenn in $f(x)$ alle Koeffizienten außer a_1 durch die Primzahl p teilbar sind, a_1 und $\frac{a_n}{p}$ nicht durch p teilbar, so ist die Gleichung $f(x) = 0$ primitiv, sofern sie irreduzibel ist.*

Perron[9]) hat die folgenden Sätze bewiesen:

Die algebraische Gleichung

$$x^n + a_1 x^{n-1} + p a_2 x^{n-2} + \dots + p a_n = 0,$$

wo $a_1, a_2, \dots, a_n$ ganze, rationale Zahlen bedeuten, deren erste und letzte durch die Primzahl p nicht teilbar sind, und wo kein Teiler von a_n (± 1 eingeschlossen) nach dem Modul p kongruent a_1 ausfällt, ist irreduzibel.

Und noch die Verallgemeinerung:

Die algebraische Gleichung

$$x^n + a_1 x^{n-1} + p^{\left[\frac{e}{n-1}\right]+1} a_2 x^{n-2} + p^{\left[\frac{2e}{n-1}\right]+1} a_3 x^{n-3} + \dots + p^{\left[\frac{(n-2)e}{n-1}\right]+1} a_{n-1} x + p^e a_n = 0,$$

wo e prim zu $n-1$ ist, und die $a_1, a_2, \dots, a_n$ genau die Bedingungen des vorigen Theorems erfüllen, ist irreduzibel.

[9]) Loc. cit. S. 453.

Es folgt jetzt unmittelbar aus meinem Satze 1, daß die Gleichungen, die hier von Perron behandelt worden sind, auch gewiß primitiv sein müssen.

§ 3.

Es soll jetzt ein etwas allgemeinerer Fall behandelt werden, indem nicht vorausgesetzt werden soll, daß h_2 zu $n - 1$ relativ prim ist, sondern daß es einen größten gemeinsamen Teiler e gibt. Dann folgt aus (7), da $\lambda_2 = \frac{n-1}{e}$ ist und $\varkappa_2 = \frac{h_2}{e}$,

$$u\,m = \tau_1 u_1' + \tau_2 \frac{n-1}{e} u_2',$$

und da wieder $u_1' = u$ ist,

$$u\,(m - \tau_1) = \tau_2 u_2' \frac{n-1}{e},$$

wo $\tau_1 = 0$ oder 1 ist. Sei erstens $\tau_1 = 0$. Dann kommt also

$$m\,u = \tau_2 u_2' \frac{n-1}{e}$$

oder, da m zu $\frac{n-1}{e}$ relativ prim ist,

$$u = k \frac{n-1}{e},$$

wo k eine ganze Zahl ist. Dies kann aber nicht für alle Primideale in (3) richtig sein, denn sonst folgt wie früher, daß der Grad von $P(\theta)$ durch $\frac{n-1}{e}$ teilbar sein muß, was nicht möglich ist. Es muß also auch ein oder mehrere u derart geben, daß $\tau_1 = 1$, also

$$u\,(m - 1) = \tau_2 u_2' \frac{n-1}{e}$$

oder, wenn der größte gemeinsame Teiler von $\frac{n-1}{e}$ und $m - 1$ gleich f ist,

$$u = k \frac{n-1}{fe}.$$

Jetzt folgt aber wie früher

$$m = (k_1 f_1 + k_2 f_2 + \ldots + k_t f_t) \frac{n-1}{fe},$$

wo k_i ganze Zahlen sind, und dies ist nicht möglich, wenn nicht $f = \frac{n-1}{e}$ ist und also $m - 1$ durch $\frac{n-1}{e}$ teilbar. Man kann dies in einem Satze so ausdrücken:

Satz 3. *Sei $f(x)$ ein irreduzibles Polynom mit einem zweiseitigen Polygon in bezug auf eine Primzahl p. Die eine Seite des Polygons soll auf der X-Achse ihre Projektion gleich* 1 *haben, und es soll für die andere*

$n-1$ und h_2 den größten gemeinsamen Faktor e besitzen. Dann sind nur solche Imprimitivitätszahlen m möglich, für welche $m-1$ durch $\frac{n-1}{e}$ teilbar ist.

m muß also von der Form $m = 1 + k\frac{n-1}{e}$ sein, wo k eine ganze Zahl ist.

§ 4.

Es soll aber ein noch allgemeinerer Satz bewiesen werden. Das Polygon soll wie früher aus r Seiten bestehen, wovon eine eine Projektion auf die X-Achse gleich 1 hat. Man darf diese Seite willkürlich wählen, also etwa $l_1 = \lambda_1 = 1$. Die Zahlen

$$\lambda_2, \lambda_3, \ldots, \lambda_r$$

sollen alle einen größten, gemeinsamen Faktor d haben. Aus der Gleichung

$$e_2\lambda_2 + e_3\lambda_3 + \ldots + e_r\lambda_r = n-1$$

schließt man, daß d auch ein Teiler von $n-1$ sein muß. Dann folgt aus (6) für diesen Fall

$$mu = \tau_1 u + \sum_{i=2}^{r} \tau_i \lambda_i u_i',$$

oder

$$(m-\tau_1)u = du',$$

wo u' eine ganze Zahl ist und τ_1 entweder 0 oder 1. Wenn $\tau_1 = 0$ ist, erhält man $um = du'$, und weil m zu d relativ prim sein muß, $u = kd$. Daraus folgt wie früher, daß n durch d teilbar ist, wenn dies für alle u der Fall wäre, was nicht möglich ist. Man hat daher für einige u $\tau_1 = 1$, folglich

$$(m-1)u = du'$$

oder

$$u = \frac{d}{e}k,$$

wo k eine ganze Zahl und e der größte gemeinsame Faktor von d und m. Dann folgt, daß n durch $\frac{d}{e}$ teilbar wird, was nur in der Weise möglich sein kann, daß $e = d$ ist, $m-1$ also durch d teilbar und folglich $m = 1 + hd$, wo h eine ganze Zahl ist

Satz 4. *Sei für das Polygon eines Polynoms $f(x)$ in bezug auf die Primzahl p die Projektion einer Seite auf die X-Achse gleich 1, und die Zahlen $\lambda_2, \lambda_3, \ldots, \lambda_r$ sollen den größten gemeinsamen Teiler d haben. Dann sind, wenn die Gleichung $f(x) = 0$ irreduzibel ist, nur solche Imprimitivitätszahlen möglich, die von der Form $m = 1 + hd$ sind, wo h eine ganze Zahl ist.*

In diesem Satze sind die früheren Sätze 1 und 3 enthalten. Man hätte noch allgemeinere Sätze beweisen können, indem man voraussetzt, daß das Polygon von $f(x)$ eine Seite hätte, die gleich 2 wäre usw. Es soll aber darauf nicht eingegangen werden, sondern nur zuletzt ein spezieller Satz bewiesen werden.

Das Polygon von $f(x)$ soll aus zwei Seiten bestehen, von denen die eine eine Projektion auf die X-Achse gleich q hat, wo q eine Primzahl $> \frac{n}{2}$ ist. Dann ist also $l_1 = n - q$ und λ_1 daher ein Teiler von $n - q$ und folglich zu n relativ-prim. In diesem Falle lautet die Gleichung (7), indem vorausgesetzt wird, daß h_2 nicht durch q teilbar ist,

$$m u = \tau_1 \lambda_1 u_1' + \tau_2 q u_2'. \tag{9}$$

Sei wie früher f_1 der größte gemeinsame Teiler von u und λ_1, dann ist

$$\lambda_1 u_1' = f_1 \lambda_1' u_1' = \lambda_1' u$$

und (9) geht in

$$(m - \tau_1 \lambda_1') u = \tau_2 q u_2'$$

über. Daraus folgt, daß entweder

$$m = \tau_1 \lambda_1'$$

ist oder u durch q teilbar, was offenbar unmöglich ist. m kann aber nicht durch λ_1' teilbar sein, ohne daß $\lambda_1' = 1$ ist, weil dann n durch λ_1' teilbar wird. Daraus folgt, daß u durch λ_1 teilbar ist, was auch nicht für alle u möglich ist, außer wenn $\lambda_1 = 1$.

Es ist also der Satz bewiesen:

Satz 5. *Sei $f(x)$ ein Polynom mit einem zweiseitigen Polygone, wo l_1 (oder l_2) eine Primzahl $> \frac{n}{2}$ ist und l_1 in h_1 nicht aufgeht. Wenn dann $f(x)$ irreduzibel ist und λ_2 nicht gleich 1, so ist $f(x)$ gleichzeitig primitiv.*

(Eingegangen am 18. Januar 1923.)

Über Kurven endlicher Ordnung.

Von

Otto Haupt in Erlangen.

§ 1.

Problemstellung.

1. Im folgenden handelt es sich, wenn von einem „*Bogen* $\mathfrak{A}$“ oder „*Bogen* $\overset{\frown}{E_1 E_2}$“ [bzw. einer „Kurve $\mathfrak{A}$“] die Rede ist, zunächst um *Jordansche Bogen* [bzw. Kurven], also um (beschränkte) ein-eindeutige, stetige Bilder einer abgeschlossenen Strecke [bzw. der Kreisperipherie] in der euklidischen Ebene $\mathfrak{E}$. Vom Falle, daß $\mathfrak{A}$ selbst eine Strecke in $\mathfrak{E}$ ist, wird grundsätzlich abgesehen; hingegen dürfen Strecken als Teilbogen von $\mathfrak{A}$ auftreten. Indes soll für die folgende Übersicht (Nr. 2 mit 4) der Einfachheit wegen das Auftreten solcher Strecken noch außer Betracht bleiben (vgl. Nr. 6).

2. In gewissem Sinne besonders einfach sind Bogen $\mathfrak{A}$ der beiden folgenden Gattungen: $\mathfrak{A}$ ist ein-eindeutiges (stetiges) Bild *entweder* eines Kreisbogens β vom Radius Eins ($0 < \beta \leqq 2\pi$) vermöge *Zentralprojektion* aus dem Zentrum Z des betrachteten Kreises (vom Radius Eins) *oder* einer Strecke vermöge *Parallelprojektion* in Richtung senkrecht zur Strecke [1]. Bogen $\mathfrak{A}$ dieser beiden Arten wollen wir im folgenden als „*relativ einfach*“ bezeichnen oder als „*einfach bezüglich* Z“ bzw. „*bezüglich der Projektionsrichtung*“.

3. Hat ein Bogen $\mathfrak{A}$ mit jedem *Halbstrahle* eines Büschels B mit dem Zentrum [2] Z bzw. mit jeder Geraden eines Parallelenbüschels B höchstens endlich viele Punkte gemeinsam, so heiße $\mathfrak{A}$ von „*endlicher Ordnung relativ* Z *bzw. relativ zur Richtung des Parallelenbüschels*“ oder kurz „*von endlicher Relativordnung*“; B heiße das „*Bezugsbüschel*“. Hat

[1] Genauere Festsetzungen in Nr. 6 (§ 2) vorliegender Arbeit.

[2] D. h. also mit allen Halbstrahlen, deren Anfangspunkt Z ist.

die Gesamtheit dieser Schnittpunktszahlen das Maximum r ($r \geqq 2$), so besitzt $\mathfrak{A}$ die „(*beschränkte*) *Relativordnung* r"; *im Falle* Z *auf* $\mathfrak{A}$ *liegt, wird* — dies sei schon hier ausdrücklich hervorgehoben — Z *bei Bestimmung von* r *als Schnittpunkt nicht mitgezählt*[3]).

Der Begriff der Relativordnung ist ersichtlich umfassender als der, in der Literatur eingeführte, Begriff der „*Ordnung (schlechthin)*"[4]). $\mathfrak{A}$ heißt nämlich von endlicher Ordnung (bzw. von der beschränkten Ordnung n), wenn $\mathfrak{A}$ von endlicher Relativordnung (bzw. von einer beschränkten Relativordnung $r \leqq n$)[5]) ist hinsichtlich eines *jeden* Punktes Z (und einer *jeden* Richtung).

4. Relativ einfache Bogen spielen eine gewisse Rolle in den Elementen der Integralrechnung, nämlich bei der Deutung des bestimmten einfachen Integrals einer in $a \leqq x \leqq b$ reellwertigen, eindeutigen, stetigen, positiven Funktion $f(x)$ als einer Maßzahl für den „Flächeninhalt" des Bereiches $a \leqq x \leqq b$, $0 \leqq y \leqq f(x)$ (x, y rechtwinklige kartesische Koordinaten). Bekanntlich beruht diese Deutung auf dem Satze, daß *jeder relativ einfache Bogen den Peano-Jordaninhalt*[6]) *Null besitzt; dies gilt allgemeiner für Bogen endlicher Relativordnung* (Satz V, § 3). Herr Rosenthal, dem ich dies Ergebnis mitteilte, machte mich darauf aufmerksam, daß der Satz als Spezialfall in einem Theorem für Lebesguesche Integrale enthalten ist, und daß er sich aufs engste berührt mit einer allgemeineren Bemerkung von Herrn Rosenthal, wonach eine Menge von endlicher oder abzählbarer Ordnung stets das innere Maß Null besitzt[7]). Wir geben in § 3 einen Beweis, für Bogen endlicher Relativordnung, der nur mit einfachen Mitteln arbeitet.

Aus der eben angegebenen Eigenschaft eines relativ einfachen Bogens folgt: Irgendein Bogen $\mathfrak{A}$ besitzt jedenfalls dann den Inhalt Null, wenn er sich als Summe von endlich vielen, relativ einfachen Bogen $\mathfrak{A}_1, \ldots, \mathfrak{A}_m$ darstellen läßt, wobei also je zwei dieser Bogen höchstens einen Endpunkt gemeinsam haben und zu jedem $\mathfrak{A}_\mu$ ein Z_μ oder eine Richtung sich an-

[3]) Genauere Festsetzungen in Nr. 7 (§ 2).

[4]) Siehe A. Rosenthal, Über die Singularitäten der reellen ebenen Kurven (Math. Annalen **73** (1913), S. 487), wo auch der Begriff der „*Ordnung einer Geraden a in bezug auf die Kurve*" eingeführt wird.

[5]) Dabei soll $r = n$ sein für mindestens ein Z oder mindestens eine Richtung.

[6]) Vgl. etwa F. Hausdorff, Grundzüge der Mengenlehre (Leipzig, 1914, Kap. X, § 2).

[7]) Siehe die inzwischen erschienene Arbeit von Herrn Rosenthal: Über Gebilde mit einzigem Ordnungsindex (Sitzungsber. d. bayer. Akad. d. W., math.-phys. Klasse, Jahrg. 1922, S. 228 und 229, Fußnote [1]). Der Satz wird dort (in unserer Ausdrucksweise gesprochen) für den Fall eines Parallelen-Bezugsbüschels bewiesen und für den Fall abzählbarer Ordnung (schlechthin) formuliert.

geben läßt, bezüglich deren $\mathfrak{A}_\mu$ relativ einfach ist ($\mu = 1, \ldots, m$). Diese Bemerkung führte zur Frage nach *einfachen, hinreichenden Bedingungen für die Zerlegbarkeit eines Bogens* $\mathfrak{A}$ *in endlich viele, relativ einfache*, insbesondere gab sie Veranlassung zur Untersuchung, *ob etwa jeder Bogen von endlicher oder wenigstens beschränkter Ordnung oder auch Relativordnung sich aus endlich vielen, relativ einfachen Bogen zusammensetzen lasse.* Ihre Beantwortung findet diese letztere Frage durch die folgenden beiden in § 2 bewiesenen Sätze:

Satz I. *Jeder Bogen* $\mathfrak{A}$ *der Relativordnung* $r \leqq 2$ *ist in endlich viele, relativ einfache Bogen zerlegbar. Hingegen lassen sich zu jeder Relativordnung* $r \geqq 3$ *Bogen angeben, die auf keine Weise als Aggregate von endlich vielen, relativ einfachen Bogen darstellbar sind.*

Satz II. *Jeder Bogen* $\mathfrak{A}$ *der Ordnung* $n \leqq 5$ *ist in endlich viele, relativ einfache Bogen zerlegbar. Hingegen gibt es Bogen von jeder Ordnung* $n \geqq 6$, *die auf keine Weise als Aggregate von endlich vielen, relativ einfachen Bogen darstellbar sind.*

Beide Sätze bleiben in Geltung, falls die beiden Endpunkte des zu zerlegenden Bogens zusammenrücken, also eine „*Kurve*" vorliegt.

Zwei einfache hinreichende Bedingungen für die Zerlegbarkeit in endlich viele, relativ einfache Bogen werden in *Satz* III *und* IV (§ 2) gegeben.

5. Die gewonnenen Ergebnisse bleiben im wesentlichen unverändert erhalten, wenn man als „Bogen" auch beschränkte, eindeutige und stetige Bilder einer abgeschlossenen Strecke (bzw. eines Kreises) zur Untersuchung zuläßt, welche „*mehrfache*" *Punkte* von höchstens „*endlichem Vielfachheitsgrade*" aufweisen[8]); dabei ist vorausgesetzt, daß die Begriffe der Ordnung und der Relativordnung geeignet festgelegt werden.

Auch auf die Bedingung der *Beschränktheit* der Bogen $\mathfrak{A}$ kann man nachträglich verzichten[9]). In der Schlußbemerkung wird auf weitere Fragestellungen hingewiesen.

§ 2.

Zerlegbarkeit in endlich viele relativ einfache Bogen.

6. *Zur Definition des Begriffes „relativ einfacher Bogen"* bemerken wir *ergänzend* folgendes: Jeder relativ einfache Bogen $\mathfrak{A}$ läßt sich darstellen in der Form $Y = f(X) \geqq 0$, $a \leqq X \leqq b$, wobei $f(X)$ eine eindeutige, reellwertige, nichtnegative, stetige Funktion der reellen Veränder-

[8]) Siehe Rosenthal, l. c.[4]), S. 481 und 487.
[9]) Siehe Rosenthal, l. c.[4]), S. 480.

lichen X bedeutet und $f(X)$ höchstens für einen einzigen Wert von X, nämlich nur entweder für $X = a$ oder aber für $X = b$ den Wert Null annehmen kann.

Deutet man nämlich X *und* Y *als Polarkoordinaten* und zwar (X: $0 \leqq a \leqq X \leqq b$, $b - a < 2\pi$) als den Bogen des Einheitskreises, Y als den Radiusvektor, so enthält der Durchschnitt der Punktmenge $\mathfrak{A}$ mit jedem Radiusvektor *einen* Punkt falls $f(a)f(b) \leqq 0$. Ist aber z. B. $f(a) = 0$, *ist also der Pol* Z des Koordinatensystems selbst *ein Punkt von* $\mathfrak{A}$, so verabreden wir sinngemäß, daß Z *nur für* $X = a$ *als* (*einziger*) *Punkt des Durchschnittes von Radiusvektor und* $\mathfrak{A}$ *mitzuzählen* ist.

Versteht man hingegen unter X, Y *rechtwinklige kartesische Koordinaten*, so enthält der Durchschnitt von $\mathfrak{A}$ mit jeder Y-Parallelen[10] ($a \leqq X \leqq b$) genau *einen* Punkt.

Wir werden also *jeden Bogen* $\mathfrak{A}$, *der sich, bezogen auf geeignet gewählte Polar- oder rechtwinklige kartesische Koordinaten, in obiger Form darstellen läßt, und nur einen solchen Bogen* $\mathfrak{A}$ *als relativ einfach bezeichnen.*

Um uns kurz ausdrücken zu können, verstehen wir von jetzt ab unter einem „*Büschel* B“: *Entweder* die Gesamtheit der von einem (im Endlichen gelegenen) Punkte Z ausgehenden *Halbstrahlen*; *oder* die Gesamtheit der Halbgeraden („*Halbstrahlen*“) einer bestimmten Richtung, welche in einer, immer auch den jeweils betrachteten Bogen $\mathfrak{A}$ enthaltenden, Halbebene verlaufen, die durch eine geeignet gewählte Gerade — oben war es die X-Achse — bestimmt wird.

Im Falle eines relativ einfachen Bogens handelt es sich um diejenigen Halbstrahlen von B, welche einen bestimmten Sektor Σ von B bilden. Wir nennen daher genauer $\mathfrak{A}$ „*relativ einfach bezüglich* Σ“ (oder auch, falls im Endlichen ein Zentrum Z vorhanden ist „*bezüglich* Z“[11]). Σ heiße ebenfalls „*Bezugsbüschel*“.

Wir lassen nunmehr auch die (bereits in Nr. 1 angekündigte) *Möglichkeit zu, daß Strecken als Teilbogen von* $\mathfrak{A}$ *auftreten.* Jetzt soll *in erweitertem Sinne* $\mathfrak{A}$ als „*relativ einfach*“ bezeichnet werden auch dann, wenn jeder Halbstrahl s eines Bezugsbüschels Σ mit $\mathfrak{A}$ höchstens entweder einen Punkt P („im gewöhnlichen Sinne“) oder eine abgeschlossene Strecke $\overline{P_1 P_2}$ (mit den Endpunkten P_1 und P_2) gemeinsam hat; die Strecke $\overline{P_1 P_2}$ soll natürlich in keiner größeren, nur aus Punkten von $\mathfrak{A}$ bestehenden Strecke als echter Teil enthalten sein. Die einzelne, auf s liegende, zu $\mathfrak{A}$

[10]) D. h. einer Parallelen zur Y-Richtung; genauer gesagt handelt es sich nur um die *Halbstrahlen* $X = \text{konst.}$, $Y \geqq 0$.

[11]) Im Falle B ein Parallelenbüschel bedeutet, sagen wir gelegentlich auch „*Z liege nicht im Endlichen*“.

gehörige Strecke bezeichnet man[12]) als „*verlängerten Punkt von* $\mathfrak{A}$ *auf* s“; sie zählt dann auf dem Halbstrahle jeweils für einen einzigen „Punkt“ von $\mathfrak{A}$. Dabei sollte es sich entweder um ein Parallelenbüschel handeln oder aber Z sollte nicht auf $\mathfrak{A}$ liegen. Liegt Z auf $\mathfrak{A}$, so heißt der Bogen wieder „*relativ einfach zu* Σ“, wenn alle Halbstrahlen des Sektors Σ mit alleiniger Ausnahme *eines* Randstrahles, *einen*, von Z verschiedenen (gewöhnlichen oder verlängerten) Punkt P mit $\mathfrak{A}$ gemeinsam haben[13]). Der Randstrahl habe nur Z mit $\mathfrak{A}$ gemeinsam [oder ev. einen verlängerten Punkt $\overline{ZP_2}$, wobei Z Endpunkt (vgl. Nr. 9) von $\mathfrak{A}$ sein soll].

7. Unter Verwendung der in Nr. 6 eingeführten Bezeichnungen *definieren wir jetzt* (vgl. Nr. 3): Ein Bogen $\mathfrak{A}$ heißt von *endlicher Relativordnung* (bzw. der *beschränkten Relativordnung* $r \geqq 2$), wenn $\mathfrak{A}$ mit jedem Halbstrahle eines Büschels B (des „*Bezugsbüschels*“) höchstens endlich viele (bzw. höchstens r und mit mindestens einem Halbstrahl auch genau r) *gewöhnliche oder verlängerte Punkte* gemeinsam hat. Im Falle *das Zentrum* Z *des Bezugsbüschels auf* $\mathfrak{A}$ liegt, wird Z *bei Bestimmung von* r *als Schnittpunkt nicht mitgezählt.*

Nach diesen Festsetzungen wenden wir uns zum *Beweise der* in Nr. 4 formulierten *Sätze* I *und* II.

Um den Gedankengang durch Einzelheiten nicht zu unterbrechen, schicken wir einige Bemerkungen voraus.

8. Jeder Bogen $\mathfrak{A}'$, welcher ganz einem, bezüglich Σ relativ einfachen Bogen $\mathfrak{A}$ (bzw. einem Bogen $\mathfrak{A}$ von der Relativordnung r bezüglich B bzw. von der Ordnung n) angehört, ist selbst relativ einfach zu Σ (bzw. von der Relativordnung $r' \leqq r$ bezüglich B bzw. von der Ordnung $n' \leqq n$).

9. Sei $\mathfrak{A}$ gegeben durch $x = h_1(t)$, $y = h_2(t)$, $0 \leqq t \leqq 1$; dabei seien $h_1(t)$ und $h_2(t)$ stetige und eindeutige Funktionen von t $(0 \leqq t \leqq 1)$. Die den Werten $t = 0$ bzw. $t = 1$ entsprechenden Punkte (im gewöhnlichen Sinne) heißen „*Endpunkte*“ *von* $\mathfrak{A}$; alle übrigen Punkte von $\mathfrak{A}$ heißen „*innere Punkte*“; jedem Punkt von $\mathfrak{A}$ entspreche nur *ein* t.

Unter einer (abgeschlossenen) *einseitigen Umgebung* $\mathfrak{U}^+$ (*bzw.* $\mathfrak{U}^-$) *von* P *auf* $\mathfrak{A}$ versteht man die Gesamtheit derjenigen Punkte von $\mathfrak{A}$, welche durch $t_0 \leqq t \leqq t_0 + \delta$ bzw. $t_0 - \delta \leqq t \leqq t_0$ geliefert werden, wobei P und t_0 einander entsprechen; δ ist eine beliebig kleine, positiv feste Größe. Unter der *Umgebung* $\mathfrak{U}$ *von* P *auf* $\mathfrak{A}$ verstehen wir die Vereinigungsmenge von $\mathfrak{U}^+$ und $\mathfrak{U}^-$. Ist P ein Endpunkt von $\mathfrak{A}$, so fällt $\mathfrak{U}$ mit $\mathfrak{U}^+$ oder mit $\mathfrak{U}^-$ zusammen. δ gibt ein Maß für die Kleinheit von $\mathfrak{U}^+$ bzw. $\mathfrak{U}^-$ bzw. von $\mathfrak{U}$.

[12]) Nach J. Hjelmslev, Contribution à la géométrie infinitésimale de la courbe réelle (Oversigt over det Kgl. Danske Vidensk. Selskabs Forh. 1911, Nr. 5, S. 469). Siehe auch Rosenthal, l. c.[4]).

Handelt es sich um einen *verlängerten Punkt* $P_1 P_2$ von $\mathfrak{A}$ auf einer Geraden g und ist $P_1 P_2$ „*innerer Punkt*“ von $\mathfrak{A}$, d. h. sind P_1 und P_2 innere Punkte von $\mathfrak{A}$ (im gewöhnlichen Sinne), so wird eine einseitige Umgebung $\mathfrak{U}^+$ oder $\mathfrak{U}^-$ (bzw. eine Umgebung $\mathfrak{U}$) von $P_1 \overline{P_2}$ auf $\mathfrak{A}$ geliefert durch Vereinigung von $\overline{P_1 P_2}$ mit einer P_2 oder P_1 nicht enthaltenden Umgebung von P_1 oder P_2 (bzw. von P_1 und P_2) auf $\mathfrak{A}$. $\overline{P_1} P_2$ heißt *Endpunkt* von $\mathfrak{A}$ auf g, wenn entweder P_1 oder P_2 Endpunkt (im gewöhnlichen Sinne) von $\mathfrak{A}$ ist; seine Umgebung besteht, abgesehen von $\overline{P_1 P_2}$, aus der nicht zu $P_1 P_2$ gehörigen einseitigen Umgebung von P_2 oder P_1.

Soweit nicht ausdrücklich anders erwähnt, kann „Punkt von $\mathfrak{A}$ auf einer Geraden“ oder „auf einem Halbstrahl“ im folgenden immer sowohl einen gewöhnlichen als einen verlängerten Punkt bedeuten.

10. Ein Punkt P von $\mathfrak{A}$ auf einer Geraden g liegt „*isoliert auf g*“, wenn eine Umgebung von P auf $\mathfrak{A}$, außer P, keinen Punkt von g enthält.

11. *Die im folgenden* (Nr. 12 mit 19) *betrachteten Bogen* unterliegen, *soweit nichts anderes bemerkt wird*, der Bedingung, daß sie *mit allen, jeweils in Frage kommenden, Geraden und Halbstrahlen je endlich viele, also lediglich isolierte Punkte gemeinsam* haben. *Dazu kommen stets die in Nr. 1 gemachten Annahmen, wobei Strecken als Teilbogen von $\mathfrak{A}$ ausdrücklich zugelassen sind* (vgl. die Festsetzung in Nr. 9 (Schluß)).

12. Es sei jetzt speziell P ein (isolierter) *innerer* Punkt von $\mathfrak{A}$ auf der Geraden g. Die beiden, durch g bestimmten, *offenen* Halbebenen seien mit $\mathfrak{H}^+$ und $\mathfrak{H}^-$ bezeichnet[13]). Hinsichtlich der gegenseitigen Lage von $\mathfrak{A}$ und g sind zwei verschiedene Fälle möglich.

Entweder finden sich in beliebig kleiner Umgebung $\mathfrak{U}$ von P auf $\mathfrak{A}$ Punkte beider Halbebenen. Eine einseitige Umgebung $\mathfrak{U}^+$ (bzw. $\mathfrak{U}^-$) von P enthält dann, von P abgesehen, nur Punkte *einer* Halbebene, also z. B. nur Punkte von $\mathfrak{H}^+$ (bzw. $\mathfrak{H}^-$). Man sagt im vorliegenden Falle: $\mathfrak{A}$ wird von g in P „*geschnitten*“ und „*P ist ein Schnittpunkt auf g*“.

Oder es finden sich in einer Umgebung von P auf $\mathfrak{A}$ nur Punkte von einer der Halbebenen. Man sagt dann: $\mathfrak{A}$ wird von g in P „*gestützt*“, „*P ist ein Stützpunkt auf g*“. Es ist dann g eine „*Grenzsekante*“[14]) von $\mathfrak{A}$.

---

[13]) D. h. die Punkte von g sind nicht mit zu $\mathfrak{H}^+$ bzw. $\mathfrak{H}^-$ gerechnet.

[14]) Hjelmslev; l. c.[12]), S. 486. Siehe auch Rosenthal, l. c.[4]), S. 487. Der Begriff der Grenzsekante ist folgendermaßen definiert: Sei t_0 ein Wert von t ($0 < t_0 < 1$) (vgl. Nr. 9); ferner (t_ν) bzw. (t'_ν) eine monoton aufsteigende (bzw. absteigende) Folge von t-Werten mit dem Limes t_0. Jede Grenzgerade derjenigen Sekanten, deren einzelne als Verbindungslinie der zu t_ν und t'_ν gehörigen Kurvenpunkte erklärt ist, heißt dann eine Grenzsekante in $P(t)$. Unter einer „Grenzsekante im verlängerten Punkt $P_1 \overline{P_2}$“ ist entsprechend die Gerade zu verstehen, welche P_1 und P_2 verbindet.

Unter Benutzung dieser Begriffe und Sätze ergeben sich nunmehr unter den in Nr. 11 gemachten Voraussetzungen folgende Tatsachen:

13. Liegen die *Endpunkte* E_1 *und* E_2 *von* $\mathfrak{A}$ *in verschiedenen Halbebenen von* g, so findet sich unter den (endlich vielen, isolierten) gemeinsamen Punkten von g und $\mathfrak{A}$ stets eine *ungerade Anzahl* von *Schnitt*punkten (und mithin mindestens *ein Schnitt*punkt).

14. *Damit ein Bogen* $\mathfrak{A}$ *in endlich viele, je relativ einfache Bogen zerlegbar sei, ist notwendig und hinreichend, daß die Umgebung eines jeden Punktes von* $\mathfrak{A}$ *in endlich viele, je relativ einfache Bogen zerlegbar ist.*

Die Bedingung ist notwendig zufolge Nr. 8; daß sie hinreicht, folgt etwa aus dem Heine-Borelschen Überdeckungssatze.

15. Es sei P *innerer* Punkt von $\mathfrak{A}$ und *Schnittpunkt* auf g; die Voraussetzungen der Nr. 11 seien erfüllt. Unter einer „*Nachbarschaft* Σ_ε *von* g“ versteht man die Gesamtheit der Halbstrahlen mit einem, *von* P *verschiedenen*[15]) Punkte Z von g als gemeinsamem Anfangspunkte, deren senkrechter Abstand α von P absolut genommen nicht größer ist als ε. Zu beliebig kleiner $\mathfrak{U}$ von P auf $\mathfrak{A}$ und jedem solchen Z auf g gehört eine Σ_ε von g derart, daß alle zu Σ_ε gehörigen Halbstrahlen (durch Z) eine ungerade Anzahl Schnittpunkte mit $\mathfrak{U}$ besitzen (Nr. 13). Auch der Fall, daß Z (auf g) nicht im Endlichen liegt (Parallelenbüschel), ist zulässig.

16. P sei *innerer Punkt* von $\mathfrak{A}$ und *Stützpunkt* auf g, so daß also (vgl. Nr. 11) eine Umgebung von P auf $\mathfrak{A}$ keine Punkte z. B. von $\mathfrak{H}^-$ enthält. Zu gegebenen, hinreichend kleinen $\mathfrak{U}^+$ und $\mathfrak{U}^-$ von P auf $\mathfrak{A}$ und zu einem gegebenen, *von* P *verschiedenen* Punkte Z von g existiert dann eine „*einseitige Nachbarschaft* Σ_ε^+ *von* g“ so daß jeder Halbstrahl von Σ_ε^+ sowohl mit $\mathfrak{U}^+$ als mit $\mathfrak{U}^-$ je eine ungerade Anzahl von P verschiedener Schnittpunkte gemeinsam hat; dabei bezeichnet Σ_ε^+ den Durchschnitt von Σ_ε mit $\mathfrak{H}^+$. Z braucht nicht notwendig im Endlichen zu liegen.

17. Schließlich sei P *Endpunkt* von $\mathfrak{A}$ und g eine Gerade durch P, so daß also nach den in Nr. 11 gemachten Annahmen eine Umgebung von P auf $\mathfrak{A}$ keine Punkte z. B. von $\mathfrak{H}^-$ enthält. Zu gegebener, hinreichend kleiner $\mathfrak{U}$ von P auf $\mathfrak{A}$ und einem beliebigen von P verschiedenen

[15]) Falls P ein verlängerter Punkt P_1P_2 ist, heißt das: Z gehört nicht zur abgeschlossenen Strecke $\bar{P}_1\bar{P}_2$. Den Abstand α messen wir dann etwa von P_1 aus. — Zwei verlängerte Punkte (auf der gleichen Geraden) sind zufolge Definition voneinander verschieden dann und nur dann, wenn die entsprechenden Strecken punktfremd sind.

Punkte Z auf g gehört dann eine Σ_z^+ [vgl. Nr. 16], so daß $\mathfrak{U}$ von jedem Halbstrahle aus Σ_z^- in einer ungeraden Zahl von Punkten geschnitten wird.

18. Nunmehr läßt sich der *Beweis des ersten Teiles von Satz* I so führen: Zufolge Nr. 14 ist alles bewiesen, wenn zu jedem Punkte eines Bogens von der Relativordnung zwei eine relativ einfache Umgebung $\mathfrak{U}^+$ sowohl als $\mathfrak{U}^-$ konstruiert werden kann.

Das *Zentrum Z des Bezugsbüschels* möge zunächst *nicht auf* $\mathfrak{A}$ liegen. Wir betrachten einen *inneren* Punkt P von $\mathfrak{A}$ und den durch P laufenden Halbstrahl s des Bezugsbüschels.

Ist P *Stützpunkt* auf s, so werden nach Nr. 16 $\mathfrak{U}^+$ und $\mathfrak{U}^-$ von allen Halbstrahlen s' des Bezugsbüschels, die zu s hinreichend, und zwar einseitig, benachbart sind, je in mindestens einem Punkte geschnitten. Da $\mathfrak{U}$ von der Relativordnung $r \leqq 2$ ist (Nr. 8), so kann es auf s' keine weiteren Schnittpunkte oder Stützpunkte geben. Überdies wird eine in $\mathfrak{U}$ enthaltene Umgebung $\mathfrak{U}_1$ von P auf $\mathfrak{A}$ durch die Gesamtheit der s' völlig überdeckt, so daß also durch jeden Punkt von $\mathfrak{U}_1$ genau ein Halbstrahl s' hindurchgeht. Folglich ist sowohl $\mathfrak{U}_1^+$ als $\mathfrak{U}_1^-$ relativ einfach zu einem passend gewählten Sektor des Bezugsbüschels.

Ist hingegen P *Schnittpunkt* auf s, so wird eine Umgebung $\mathfrak{U}$ von P auf $\mathfrak{A}$ von allen, zu s genügend benachbarten Halbstrahlen s'' des Bezugsbüschels in einer ungeraden Anzahl von Punkten geschnitten, also nur in je einem Punkte, weil die Relativordnung von $\mathfrak{U}$ höchstens zwei ist. Neben diesem Schnittpunkte können auf s'' Stützpunkte nicht auftreten (Nr. 16). Man schließt wie oben, daß eine hinreichend kleine Umgebung von P relativ einfach ist bezüglich Z.

Ganz entsprechend erledigt sich nach Nr. 17 der Fall eines *Endpunktes P*.

Jetzt möge das *Zentrum Z des Bezugsbüschels auf* $\mathfrak{A}$ *liegen*. Es genügt die Betrachtung des Falles, daß Z *Endpunkt von* $\mathfrak{A} = \overset{\frown}{E_1 E_2}$ ist, da wir andernfalls ja Z als Endpunkt der beiden Teilbogen $\overset{\frown}{E_1 Z}$ und $\overset{\frown}{E_2 Z}$ von $\mathfrak{A}$ auffassen können, deren jeder von der Relativordnung $r \leqq 2$ sein muß.

Da für die von Z verschiedenen Punkte von $\mathfrak{A}$ die obigen Überlegungen in Geltung bleiben, so ist nur noch zu zeigen, daß Z Endpunkt eines relativ einfachen Teilbogens von $\mathfrak{A}$ ist. Wir dürfen überdies annehmen, daß Z *keiner, ganz in* $\mathfrak{A}$ *liegenden Strecke angehört*, da ja andernfalls eben diese Strecke bereits eine relativ einfache Umgebung von Z auf $\mathfrak{A}$ wäre.

Wir können und wollen jetzt einen Halbstrahl s_1 des Bezugsbüschels so gewählt denken, daß s_1 mit $\mathfrak{A}$ mindestens einen weiteren von Z verschiedenen (isolierten) Punkt gemeinsam hat. Der Bogen $\mathfrak{B} = \overset{\frown}{ZP}$ sei

die kleinste (einseitige) Umgebung von Z auf $\mathfrak{A}$, deren, von Z verschiedener, Endpunkt P auf s_1 liegt. Wir nehmen zunächst an, es gebe einen von s_1 verschiedenen Halbstrahl t des Bezugsbüschels, welcher mit $\mathfrak{B}$ zwei und nur zwei, untereinander, sowie von Z und P verschiedene, Punkte Q und R gemeinsam hat[16]). Wir dürfen voraussetzen, daß Q und R Schnittpunkte sind. Denn wäre auch nur einer von ihnen Stützpunkt auf t, so gebe es nach Nr. 16 Nachbarstrahlen t' von t, für welche (mindestens) einer der Stützpunkte in (mindestens) zwei untereinander und von Z und P verschiedene Schnittpunkte R' und Q' aufgelöst ist; da $\mathfrak{A}$ von der Relativordnung 2 ist, enthält also t' außer R' und Q' keine weiteren, von Z verschiedenen Punkte von $\mathfrak{A}$, und es kann t' an Stelle von t der weiteren Betrachtung zugrunde gelegt werden. Liegt etwa R auf $\mathfrak{B}$ „zwischen“[17]) Z und Q, so verläuft der Bogen $\mathfrak{C}_1 = \overset{\frown}{PQ}$ in einem bestimmten, durch s_1 und t gebildeten „abgeschlossenen“[18]) Winkelraume $\mathfrak{w}$, der Bogen $\mathfrak{C}_2 = \overset{\frown}{QR}$ verläuft, von Q und R abgesehen, außerhalb $\mathfrak{w}$, schließlich liegt $\mathfrak{C}_3 = \overset{\frown}{RZ}$ wieder ganz in $\mathfrak{w}$. Die in $\mathfrak{w}$ verlaufenden Halbstrahlen des Bezugsbüschels bilden den „abgeschlossenen“ Sektor Σ. Nun wird $\mathfrak{C}_1$ von jedem Halbstrahle s^* aus Σ in einer ungeraden Anzahl von Punkten, mindestens in einem Punkte geschnitten, wenn wir von den Randstrahlen s_1 und t absehen (Nr. 13). Es kann aber nur einen Schnittpunkt geben, weil $\mathfrak{C}_1$ nach Voraussetzung und nach Nr. 8 von einer Relativordnung $r \leqq 2$ bezüglich Σ. Demzufolge hat $\mathfrak{C}_3$ mit s^* höchstens einen Punkt gemeinsam, welcher übrigens (zufolge Nr. 16) ein Schnittpunkt auf s^* sein muß. $\mathfrak{C}_3$ wird von Σ völlig überdeckt.

Jetzt schließt man in folgender Weise auf die Existenz eines ganz zu Σ gehörigen (abgeschlossenen) Sektors Σ_2 des Bezugsbüschels, relativ zu welchem $\mathfrak{C}_3$ einfach ist. Vermittelst fortgesetzter Halbierung von Σ ergibt sich zunächst die Existenz eines von t verschiedenen Strahles s_0 von Σ, so beschaffen, daß einerseits (falls $s_0 \neq s_1$) in dem von s_1 und s_0 begrenzten, abgeschlossenen Teilsektor Σ_1 von Σ kein Strahl mit $\mathfrak{C}_3$ einen, von Z verschiedenen, Punkt gemeinsam hat, während andrerseits in beliebig kleiner, einseitiger Nachbarschaft von s_0 noch Strahlen s^* von Σ auftreten, welche mit $\mathfrak{C}_3$ einen von Z verschiedenen Punkt gemeinsam haben. In dem von s_0 und t begrenzten Teilsektor Σ_2 von Σ muß jetzt aber über-

[16]) Es sei hier an die in Nr. 7 getroffene Verabredung erinnert, derzufolge, falls Z auf $\mathfrak{A}$ liegt, Z bei der Bestimmung der Relativordnung von $\mathfrak{A}$ nicht mitgezählt wird.

[17]) D. h. ist $\tau_Z < \tau_R < \tau_Q < \tau_P$ oder $\tau_Z > \tau_R > \tau_Q > \tau_P$, wenn τ_Z usw. die den Punkten Z usw. entsprechenden Parameterwerte von τ bedeuten, falls $\mathfrak{A}$ gegeben ist (vgl. Nr. 9) durch $x = h_1(\tau)$, $y = h_2(\tau)$, $0 \leqq \tau \leqq 1$.

[18]) D. h. die Punkte der „Randstrahlen“ s und t — einschließlich Z — gehören zu $\mathfrak{w}$.

haupt jeder Halbstrahl s^* (ausgenommen s_0) einen (und nur einen) von Z verschiedenen Punkt von $\mathfrak{C}_3$ enthalten, weil andernfalls Z mehrfacher Punkt von $\mathfrak{C}_3$ wäre.

Die anfangs beiseite gelassene Annahme, daß bereits $\mathfrak{B}$ von jedem Halbstrahle des Bezugsbüschels in höchstens einem, von Z verschiedenen Punkte getroffen werde, erledigt sich durch die gleichen Überlegungen, welche wir soeben auf $\mathfrak{C}_3$ angewandt haben.

19. Mit Hilfe der Resultate von Nr. 18 gelingt der *Beweis des ersten Teiles von Satz* II.

Für die *Bogen* $\mathfrak{A}^{(3)}$ *der Ordnung* 3 ist der Satz trivial. Denn sei Z ein Punkt von $\mathfrak{A}^{(3)}$; dann hat nach Voraussetzung jede Gerade, und um so mehr jeder Halbstrahl mit dem Anfangspunkte Z, höchstens zwei Punkte außer Z mit $\mathfrak{A}^{(3)}$ gemeinsam: d. h. $\mathfrak{A}^{(3)}$ ist von der Relativordnung $r \leqq 2$ bezüglich Z[16]).

Für die *Bogen* $\mathfrak{A}^{(4)}$ *bzw.* $\mathfrak{A}^{(5)}$ *der Ordnungen* 4 *bzw.* 5 schließen wir so: Sei P irgendein Punkt von $\mathfrak{A}$; wir können vom Falle absehen, daß P im Innern einer ganz zu $\mathfrak{A}$ gehörigen Strecke liegt. *Entweder* ist eine Umgebung von P auf $\mathfrak{A}$ von der Relativordnung $r \leqq 2$ bezüglich P; dann ist eine Umgebung von P in endlich viele relativ einfache Bogen zerlegbar (Nr. 18). *Oder* es existiert zu einer (sogar beliebig kleinen) Umgebung $\mathfrak{U}$ von P auf $\mathfrak{A}$ mindestens ein Halbstrahl s mit dem Anfangspunkte P, welcher mit $\mathfrak{U}$ mindestens drei, untereinander und von P verschiedene, innere Punkte von $\mathfrak{U}$ gemeinsam hat; sie seien Q, R und S.

Sind alle drei Punkte Schnittpunkte auf s und ist P Schnittpunkt (bzw. Stützpunkt bzw. Endpunkt) von $\mathfrak{A}$ auf s, so wird nach Nr. 15 (bzw. Nr. 16 bzw. Nr. 17) eine (im Falle P Endpunkt ist, einseitige) Umgebung $\mathfrak{U}_1$ von P in mindestens einem (bzw. mindestens zwei bzw. mindestens einem) von P verschiedenen Punkte geschnitten von jeder zu s hinreichend benachbarten (bzw. einseitig benachbarten) Parallelen von s; andrerseits entspricht jedem der Punkte Q, R und S je eine ungerade Anzahl Schnittpunkte, mindestens aber *ein* Schnittpunkt von $\mathfrak{A}$ auf jeder dieser Nachbarparallelen zu s. Bei genügender Einschränkung dieser Nachbarschaft hat man also auf jeder Parallelen mindestens drei untereinander verschiedene und nicht zu $\mathfrak{U}_1$ gehörige Schnittpunkte mit $\mathfrak{A}$. Folglich ist eine in $\mathfrak{U}_1$ enthaltene Umgebung von P von der Relativordnung $r \leqq 2$ (bezüglich eines Parallelenbüschels). Aus Nr. 18 ergibt sich jetzt die Behauptung.

Findet sich dagegen unter den Punkten Q, R und S mindestens je ein Schnittpunkt und ein Stützpunkt, so gibt es auf einem passend gewählten, zu s benachbarten Halbstrahl durch P nach Nr. 15 und 16 mindestens drei von P verschiedene Schnittpunkte Q_1, R_1 und S_1 und wir

kommen wieder auf den eben behandelten Fall zurück. Entsprechend schließt man, falls Q, R und S sämtlich Stützpunkte auf s sein sollten.

20. Den *zweiten Teil von Satz* I *und* II erledigen wir durch *Konstruktion eines Beispiels*, nämlich eines Bogens $\mathfrak{B}_0$, welcher *einerseits von der Ordnung* 6 *und — bezüglich eines seiner Punkte — von der Relativordnung* 3 *ist, andrerseits aber sich auf keine Weise in endlich viele, relativ einfache Bogen zerlegen läßt.*

Es seien x und y rechtwinklige, kartesische Koordinaten. Wir markieren auf dem Kreisbogen $0 \leqq x \leqq 1$, $y = \sqrt{1 - x^2}$ die Punkte $P_\nu(x_\nu, y_\nu)$ mit $x_\nu = 1 - \frac{1}{\nu}$, $y_\nu = \sqrt{1 - x_\nu^2}$ $(\nu = 1, 2, 3, \ldots)$. Die Sehne $\overline{P_\nu P_{\nu+1}}$ begrenzt mit dem über ihr stehenden Kreisbogen $\beta_\nu < \frac{\pi}{2}$ das Segment σ_ν $(\nu = 1, 2, \ldots)$.[19]) Um $\mathfrak{B}_0$ zu erhalten, verbinden wir jetzt P_ν mit $P_{\nu+1}$ durch einen ganz im Innern oder auf der Begrenzung von σ_ν verlaufenden Bogen $\mathfrak{b}_\nu$, den wir folgendermaßen definieren: Es sei M_ν der Mittelpunkt von β_ν, $\mathfrak{k}_\nu$ der dem Dreieck $P_\nu M_\nu P_{\nu+1}$ eingeschriebene Kreis; die Dreieckseiten $P_\nu M_\nu$ bzw. $M_\nu P_{\nu+1}$ bzw. $P_{\nu+1} P_\nu$ werden von $\mathfrak{k}_\nu$ berührt in den Punkten S_ν bzw. T_ν bzw. Q_ν. Dann besteht $\mathfrak{b}_\nu$ aus den abgeschlossenen Strecken $\overline{P_\nu S_\nu}$ und $\overline{T_\nu P_{\nu+1}}$ sowie aus dem Kreisbogen $\overset{\frown}{S_\nu Q_\nu T_\nu}$. Die von sämtlichen $\mathfrak{b}_\nu$ unter Hinzunahme des Punktes P_∞ $(x = 1,\ y = 0)$ gebildete Punktmenge $\mathfrak{B}_0$ ist ein Jordanbogen und insbesondere von der gewünschten Beschaffenheit.

Denn zunächst ist $\mathfrak{B}_0$ von der Ordnung 6. Zwar ist jeder Bogen $\mathfrak{b}_\nu$ für sich von der Ordnung 4; aber $\mathfrak{b}_\nu$ wird nur von solchen Geraden in vier Punkten getroffen, welche — abgesehen höchstens von P_ν und $P_{\nu+1}$ — mit keinem weiteren σ_μ bzw. $\mathfrak{b}_\mu$ $(\mu \neq \nu)$ Punkte gemeinsam haben. Ferner enthält irgendeine Gerade der Ebene — wenn man von den Punkten P_ν absieht — innere Punkte oder Randpunkte von höchstens zwei verschiedenen der σ_ν; sie trifft also $\mathfrak{B}_0$ in höchstens sechs Punkten, und diese Maximalzahl von gemeinsamen Punkten wird auch wirklich erreicht. Schließlich folgt noch, daß $\mathfrak{B}_0$ von der Relativordnung 3 ist z. B. bezüglich des Punktes P_∞.

$\mathfrak{B}_0$ bzw. irgendeine Umgebung von P_∞ läßt sich nicht in endlich viele, relativ einfache Bogen zerlegen. Denn ist irgendein Halbstrahlenbüschel gegeben mit beliebigem (im Endlichen oder nicht im Endlichen gelegenen) Zentrum, so wird jede beliebig kleine (einseitige) Umgebung von P_∞ auf $\mathfrak{B}_0$ durch Halbstrahlen des Büschels in drei, von P_∞ verschiedenen Punkten getroffen.

---

[19]) Die Verwendung einer solchen Segmentenfolge (zu ganz ähnlichen Zwecken) nach Hjelmslev, l. c.[12]), S. 492.

Die Konstruktion von *Bogen höherer als 6. Ordnung bzw. höherer als 3. Relativordnung, die sich nicht in endlich viele, relativ einfache Bogen zerlegen lassen*, kann etwa so erfolgen:

Um einen Bogen 7. Ordnung zu erhalten, fügt man zu $\mathfrak{B}_0$ noch eine Strecke $0 \leqq x \leqq a$, $y = 1$ hinzu. Einen Bogen 8. Ordnung (allgemein $2n$-ter Ordnung) erhält man aus $\mathfrak{B}_0$, wenn man an Stelle der beim Aufbau von $\mathfrak{B}_0$ benutzten Bogen b_ν geeignet gewählte Bogen 4. Ordnung (bzw. n-ter Ordnung) treten läßt usw.

21. Die in P_ν, S_ν und T_ν auftretenden Ecken bzw. Spitzen können wir abrunden (etwa durch Einfügen passend gewählter Kreisbogen), ohne dadurch die für uns hier wesentlichen Eigenschaften von $\mathfrak{B}_0$ preiszugeben[20]. Wir erhalten so aus $\mathfrak{B}_0$ einen „*gewöhnlichen Bogen*" $\mathfrak{B}^*$, d. h. einen Bogen, dessen sämtliche Punkte „*gewöhnliche differenzierbare Stellen*" sind[21]. Darunter ist folgendes zu verstehen: Es sei $\mathfrak{B}^*$ gegeben durch $x = h_1(t)$, $y = h_2(t)$, $0 \leqq t \leqq 1$, $[h_1(0) = 1,\ h_2(0) = 0]$, bezogen auf rechtwinklige kartesische Koordinaten x, y. Für jedes τ $(0 < \tau < 1)$ gilt dann:

$$\Theta_j(\tau) = \lim_{t \to \tau - 0} \frac{\Delta h_j}{\varrho} = -\lim_{t \to \tau - 0} \frac{\Delta h_j}{\varrho}, \quad j = 1, 2;$$

dabei ist $\Delta h_j = h_j(t) - h_j(\tau)$; $\varrho = +\sqrt{(\Delta h_1)^2 + (\Delta h_2)^2}$.

Für die Intervallendpunkte wird natürlich nur die Existenz der Grenzwerte in *einer* Richtung gefordert[22]. Jede Stelle $t = \tau$, wo Θ_1 und Θ_2 insbesondere stetig sind, heißt eine „*gewöhnliche*) *stetig differenzierbare Stelle*"[23]. Alle Punkte von $\mathfrak{B}^*$ sind stetig differenzierbare Stellen mit Ausnahme von P_x.

Etwas allgemeiner ist folgendes Verhalten der Tangente eines gewöhnlichen Bogens, welches stetige Differenzierbarkeit als Spezialfall umfaßt: In einer Umgebung der Stelle $t = \tau_0$ schwankt die Richtung der Tangente um weniger als π. Das soll heißen: Um $t = \tau_0$ läßt sich eine Umgebung $t - \tau_0 \leqq \delta$ abgrenzen, in welcher $\Phi(t; \tau_0) = \Theta_1(t)\,\Theta_1(\tau_0) + \Theta_2(t)\,\Theta_2(\tau_0)$ positiv (größer als Null) bleibt. Wir wollen in diesem Falle sagen, der Bogen besitze im Punkte $t = \tau_0$ eine „*Tangente von kleiner Oszillation*". Jetzt sieht man, daß der oben konstruierte Bogen $\mathfrak{B}^*$ hinsichtlich der

[20]) Auch die Rektifizierbarkeit von $\mathfrak{B}_0$ kann gleichzeitig erzwungen werden.

[21]) Siehe Hjelmslev, l. c.[12]), S. 447 und 449; sowie Rosenthal, l. c.[4]), S. 482. Daß P_x eine (einseitig) differenzierbare Stelle ist, folgt schon aus dem allgemeinen Satze, wonach jeder Bogen endlicher Ordnung überall vorn und hinten differenzierbar ist. Siehe Rosenthal, l. c.[4]), S. 516.

[22]) Also nur z. B. die Existenz (und folglich Endlichkeit) von $\lim_{t \to \tau - 0} \frac{\Delta h_j}{\varrho}$.

[23]) Rosenthal, l. c.[4]), S. 483.

Existenz und Stetigkeit der Tangente in gewissem Sinne das Äußerste leistet, was man verlangen kann. Es gilt nämlich der

Satz III. *Damit ein gewöhnlicher Bogen $\mathfrak{C}$ in endlich viele, relativ einfache Bogen zerlegbar sei, ist hinreichend, daß $\mathfrak{C}$ in jedem Punkte eine Tangente kleiner Oszillation besitze*[24]). $\mathfrak{C}$ braucht dabei keineswegs von endlicher Ordnung zu sein.

Man bemerke, daß der gewöhnliche Bogen $\mathfrak{B}^*$ in P_∞ keine Tangente kleiner Oszillation besitzt. Zum Beweise des Satzes betrachten wir einen Punkt $t = \tau_0$ von $\mathfrak{C}$ und eine, nach Voraussetzung vorhandene, Umgebung $\mathfrak{U}$ dieses Punktes, für welche $\Phi(t, \tau_0) \neq 0$. Wäre jetzt $\mathfrak{U}$ nicht relativ einfach z. B. bezüglich der Normalenrichtung im Punkte $t = \tau_0$, so würde $\mathfrak{U}$ mit (mindestens) einer Parallelen zu dieser Richtung mindestens zwei voneinander verschiedene Punkte, P und Q, gemeinsam haben. Es müßte somit auf dem Bogen $\overset{\frown}{PQ}$, also in $\mathfrak{U}$, an mindestens einer Stelle $t = t^*$ die Beziehung $\Phi(t^*; \tau_0) = 0$ gelten[25]), gegen die Voraussetzung.

Wir bemerken noch, daß sich ein gewöhnlicher Bogen $\mathfrak{C}$ von der im Satz III angegebenen Eigenschaft in endlich viele, relativ einfache Bogen zerlegen läßt lediglich unter Benutzung von Parallelenbüscheln oder allgemeiner gesprochen von Büscheln, deren Zentra sämtlich auf einer ($\mathfrak{C}$ nicht schneidenden) Geraden liegen. Darin liegt bereits eine Besonderheit: das folgt aus der Existenz von *Bogen, die relativ einfach sind nur bezüglich eines einzigen Punktes bzw. Büschels.*

Beispiel. $y = {}_+\sqrt{x}\sin\frac{1}{x}$, $0 < x \leqq 1$; $y = 0$, $x = 0$ (x, y bedeuten rechtwinklige kartesische Koordinaten). Dieser Bogen ist relativ einfach lediglich bezüglich des Büschels aus Parallelen zur y-Richtung. Man kann dies etwa so einsehen: Betrachtet man ein Büschel, dessen Zentrum Z nicht der y-Achse angehört, so liegt auf dem Strahle durch den Koordinatenanfangspunkt der Punkt P_0 ($x = 0$, $y = 0$) des betrachteten Bogens nicht isoliert. Liegt aber Z ($x = 0$, $y = a$) auf der y-Achse, so gibt es in beliebig kleiner Umgebung von P_0 noch Tangenten des Bogens, deren Abschnitte auf $x = 0$ sowohl größer als auch kleiner sind als a[26]). Folglich geht von Z an die genannte Umgebung mindestens eine Tangente, die nicht Wendetangente ist; woraus dann die Existenz von Büschelstrahlen folgt, die mindestens drei verschiedene Punkte mit jener Umgebung gemeinsam haben.

[24]) Für den Fall eines „gewöhnlichen Linienstückes", d. h. unter der Voraussetzung, daß $h_1(t)$ und $h_2(t)$ stetig differenzierbar sind und $[h_1'(t)]^2 + [h_2'(t)]^2 \neq 0$, $0 \leqq t \leqq 1$, findet sich der Satz bewiesen bei H. v. Mangoldt, Einführung in die höhere Mathematik (Leipzig 1920, 2. Aufl., 3. Bd., S. 190).

[25]) Hjelmslev, l. c.[12]), S. 450, Théorème 9.

[26]) a ist eine beliebige reelle Konstante.

22. Im Vorangehenden hatte sich gezeigt, daß ein Bogen von *beschränkter Ordnung* im allgemeinen nicht in endlich viele, relativ einfache Bogen zerlegbar ist. Demgegenüber gilt

Satz IV. *Ein Bogen $\mathfrak{A}$ ist sicher dann in endlich viele, relativ einfache Bogen zerlegbar, wenn die Klasse eines einzigen Punktes Z der Ebene oder die Klasse einer einzigen Richtung endlich ist bezüglich $\mathfrak{A}$.*

Dabei *heißt ein Punkt Z der Ebene (bzw. eine Richtung $\mathfrak{R}$) von endlicher Klasse*[27]) *bezüglich $\mathfrak{A}$*, wenn es *nur endlich viele Grenzsekanten von $\mathfrak{A}$* gibt, welche *durch Z gehen* (bzw. welche *zu $\mathfrak{R}$ parallel* sind).

Für den Fall, daß Z auf $\mathfrak{A}$ liegt, hat bereits Herr Hjelmslev[28]) bemerkt, daß — in unserer Terminologie — die Umgebung von Z auf $\mathfrak{A}$ in (endlich viele) zu Z relativ einfache Bogen zerfällt, falls von Z aus nur endlich viele Grenzsekanten an $\mathfrak{A}$ gehen. Wir begnügen uns hier mit dem Hinweis auf die einschlägigen Überlegungen von Herrn Hjelmslev, die auch zum Ziele führen, falls Z nicht auf $\mathfrak{A}$ liegt; zu bemerken ist nur, daß *im obigen Satze zwei Grenzsekanten s_1 und s_2 auch dann als „verschieden" zu bezeichnen sind, wenn zwar s_1 sowohl als s_2 auf der nämlichen Geraden liegen, aber s_1 bzw. s_2 Grenzsekanten in verschiedenen Punkten von $\mathfrak{A}$ sind.*

§ 3.

Inhalt der Bogen endlicher Relativordnung.

23. Es handelt sich um den in Nr. 4 erwähnten Beweis von

Satz V. *Jeder Bogen $\mathfrak{B}$ von endlicher Relativordnung besitzt den Peano-Jordaninhalt Null.*

Es genügt, den Gedankengang für den Fall zu skizzieren, daß $\mathfrak{B}$ von endlicher Ordnung ist relativ der y-Richtung, wobei wieder x, y rechtwinklige kartesische Koordinaten bedeuten.

Zum Beweise von Satz V ist nur zu zeigen, daß der äußere Inhalt $\varphi(\mathfrak{B})$ von $\mathfrak{B}$ Null ist. Sei $\mathfrak{B}$ gegeben durch $x = h_1(t)$, $y = h_2(t)$, $0 \leqq t \leqq 1$, wobei wir annehmen können, daß $0 \leqq h_1(t) \leqq 1$, $0 \leqq h_2(t) \leqq 1$ ist. Wir betrachteten die beiden abgeschlossenen Teilmengen $\mathfrak{B}_1^{(1)}$ und $\mathfrak{B}_1^{(2)}$ von $\mathfrak{B}$, welche definiert sind durch die Bedingungen $0 \leqq x \leqq \frac{1}{2}$ bzw. $\frac{1}{2} \leqq x \leqq 1$. Ihre äußeren Inhalte $\varphi(\mathfrak{B}_1^{(1)})$ und $\varphi(\mathfrak{B}_1^{(2)})$ stehen zu $\varphi(\mathfrak{B})$ in der Relation[29])

$$\varphi(\mathfrak{B}) \leqq \varphi(\mathfrak{B}_1^{(1)}) + \varphi(\mathfrak{B}_1^{(2)}),$$

---

[27]) Rosenthal, l. c.[4]) S. 487.

[28]) Hjelmslev, l. c.[12]), S. 492, Théorème 32, letzter Satz.

[29]) Vgl. Hausdorff, l. c.[6]), S. 404.

weil der Durchschnitt von $\mathfrak{B}_1^{(1)}$ und $\mathfrak{B}_1^{(2)}$ den Inhalt Null hat. Infolgedessen gilt für eine der Teilmengen, z. B. für $\mathfrak{B}_1^{(1)} = \mathfrak{B}_1$:

$$\varphi(\mathfrak{B}_1) \geqq 2^{-1}\varphi(\mathfrak{B}).$$

Die gleiche Überlegung führt von $\mathfrak{B}_1$ zu einer abgeschlossenen Teilmenge $\mathfrak{B}_2$ von $\mathfrak{B}_1$, für welche

$$\varphi(\mathfrak{B}_2) \geqq 2^{-2}\varphi(\mathfrak{B}).$$

Und so fortfahrend gelangt man zu einer in $0 \leqq x \leqq 1$ gelegenen Intervallschachtelung $i_1, i_2, \ldots$, welche eindeutig eine y-Parallele $x = \xi$ definiert. i_n hat die Länge 2^{-n}, für die zu i_n gehörige Teilmenge $\mathfrak{B}_n$ gilt

$$\varphi(\mathfrak{B}_n) \geqq 2^{-n}\varphi(\mathfrak{B}). \tag{1}$$

Anderseits ist, wie noch gezeigt wird, für fast alle n

$$2^{-n} \cdot \varepsilon \geqq \varphi(\mathfrak{B}_n), \tag{2}$$

unter ε eine beliebig kleine, vorgegebene, positive Zahl verstanden. Aus (1) und (2) folgt dann $\varphi(\mathfrak{B}) = 0$.

Die Ungleichung (2) ist Folge der endlichen Relativordnung von $\mathfrak{B}$. Die y-Parallele $x = \xi$ hat nämlich mit $\mathfrak{B}$ nur endlich viele, etwa im ganzen M, verschiedene Punkte gemeinsam; diese wollen wir zunächst als gewöhnliche Punkte voraussetzen und ihre Ordinaten mit $y_1, y_2, \ldots, y_M$ $(0 \leqq y_1 < y_2 < \ldots < y_M \leqq 1)$ bezeichnen. Wegen der Beschränktheit und Abgeschlossenheit von $\mathfrak{B}$ existiert zu jedem $\delta > 0$ eine natürliche Zahl $N(\delta)$ so beschaffen, daß $\mathfrak{B}_n$ enthalten ist in der Punktmenge

$$\xi - 2^{-n} \leqq x \leqq \xi + 2^{-n}, \quad y_\mu - \delta \leqq y \leqq y_\mu + \delta, \quad \mu = 1, 2, \ldots, M,$$

für alle $n > N(\delta)$; dabei soll aber 2δ kleiner sein als die kleinste der Differenzen $y_\varrho - y_{\varrho-1}$ $(\varrho = 2, 3, \ldots, M)$. Daraus folgt

$$\varphi(\mathfrak{B}_n) \leqq M \cdot 2\delta \cdot 2 \cdot 2^{-n} = 2^{-n} \cdot 4M\delta \quad \text{für} \quad n > N(\delta), \text{ w. z. b. w.}$$

Und entsprechend schließt man, wenn unter den auf $x = \xi$ gelegenen Punkten von $\mathfrak{B}$ auch verlängerte Punkte vorkommen.

Der Fall eines Bezugsbüschels mit im Endlichen gelegenem Zentrum erledigt sich in gleicher Weise.

Schluß.

24. Die Ergebnisse des § 2 lehren, daß bei den Bogen der Relativordnung $r \geqq 3$ bzw. der Ordnung $n \geqq 6$ — im Gegensatz zu den Bogen der Relativordnung $r = 2$ bzw. der Ordnung $n \leqq 5$ — als wesentlich neue Elemente solche Bogen auftreten können, welche nicht in endlich viele, relativ einfache Bogen zerlegbar sind. Derartig unzerlegbare Bogen

lassen sich wiederum klassifizieren hinsichtlich ihrer *Zerlegbarkeit in endlich viele Bogen niedrigerer Relativordnung*, woran sich weitere Fragestellungen knüpfen.

25. Bei einem vorgelegten Bogen $\mathfrak{A}^{(II)}$ der Relativordunng 2 kann die — immer mögliche — Zerlegung in endlich viele, relativ einfache Bogen im allgemeinen auf mannigfach verschiedene Art vorgenommen werden. Unter diesen Zerlegungen betrachten wir diejenigen, bei welchen die Anzahl der relativ einfachen Teilbogen von $\mathfrak{A}^{(II)}$ den kleinsten Wert $m(\mathfrak{A}^{(II)})$ besitzt. Der Gesamtheit aller möglichen $\mathfrak{A}^{(II)}$ entspricht die Menge der zugehörigen $m(\mathfrak{A}^{(II)})$. Diese hat, wie sich zeigen läßt, ein Maximum $m(II)$; m. a. W.: *Irgendein* $\mathfrak{A}^{(II)}$ *ist immer in* $m(II)$ *relativ einfache Bogen zerlegbar. Wie liegen in dieser Hinsicht die Verhältnisse bei den Bogen der Ordnungen* 4 *und* 5?

26. Weitere Fragen stellte Herr Tietze in Unterhaltungen über die Ergebnisse vorliegender Arbeit. Diese Fragen betreffen einmal die Verallgemeinerung auf Räume höherer Dimension, ferner die Übertragung des Begriffes der Relativordnung auf allgemeinere „Koordinatensysteme“[30]).

Wir gehen auf all dies hier nicht mehr ein.

Erlangen, Math. Seminar d. Universität, 30. Januar 1923.

---

[30]) Siehe auch Rosenthal, l. c. [7]).

(Eingegangen am 3. Februar 1923.)

Über Gitterpunkte in mehrdimensionalen Ellipsoiden.

Von

Arnold Walfisz in Wiesbaden.

Es sei $x > 0$, $k \geqq 2$ ganz;

$$Q = \sum_{\mu,\nu=1}^{k} a_{\mu\nu} u_\mu u_\nu \qquad (a_{\mu\nu} = a_{\nu\mu})$$

eine positiv definite quadratische Form mit beliebigen reellen Koeffizienten und der Determinante D.

Für die Summe der mit den Gewichten

$$e^{2\pi i(\alpha_1 m_1 + \ldots + \alpha_k m_k)}$$

($\alpha_1, \ldots, \alpha_k$ beliebig reell) belasteten Gitterpunkte im k-dimensionalen Ellipsoid $Q \leqq x$ bewies E. Landau i. J. 1915 [1])

$$(1) \qquad \sum_{Q \leqq x} e^{2\pi i(\alpha_1 m_1 + \ldots + \alpha_k m_k)} = \delta \frac{\pi^{\frac{k}{2}}}{\sqrt{D}\,\Gamma\left(\frac{k}{2}+1\right)} x^{\frac{k}{2}} + O\left(x^{\frac{k}{2} - \frac{k}{k+1}}\right),$$

wobei $\delta = 1$ oder $= 0$, je nachdem alle α ganzzahlig sind oder nicht.

---

[1]) E. Landau, I. „Zur analytischen Zahlentheorie der definiten quadratischen Formen (Über die Gitterpunkte in einem mehrdimensionalen Ellipsoid)“, Berliner Akademieberichte 1915, S. 458–476; II. „Über eine Aufgabe aus der Theorie der quadratischen Formen“, Wiener Sitzungsberichte, Abt. IIa, **124** (1915), S. 445–468; III. „Über die Anzahl der Gitterpunkte in gewissen Bereichen (zweite Abhandlung)“, Göttinger Nachrichten 1915, S. 209–243. In einer älteren Arbeit IV. „Über die Anzahl der Gitterpunkte in gewissen Bereichen“, Göttinger Nachrichten 1912, S. 687–771 kommt Landau, in etwas engerem Rahmen (ganzzahlige $a_{\mu\nu}$), bis zum Exponenten $\left(\frac{k}{2} - \frac{k}{k+1} + \varepsilon\right)$ im O-Glied. Die in I bis IV zur Anwendung gelangende Methode gehört der komplexen Funktionentheorie an.

Einen Beweis von (1) für den Spezialfall ganzzahliger $\alpha_1, \ldots, \alpha_k$ mit den Hilfsmitteln der reellen Analysis (Pfeiffersche Methode) erbrachte J. G. van der Corput, „Over definiete kwadratische vormen“, Niew Archief voor Wiskunde **13** (1919), S. 125–140.

Setzt man in (1)

$$\alpha_1 = 0, \ldots, \alpha_k = 0; \quad \delta = 1; \quad Q = u_1^2 + \ldots + u_k^2; \quad D = 1,$$

d. h. spezialisiert man auf Gitterpunkte mit dem Gewicht 1 in einer k-dimensionalen Kugel, so kommt

$$(2) \qquad F_k(x) = \sum_{m_1^2 + \ldots + m_k^2 \leqq x} 1 = \frac{\pi^{\frac{k}{2}}}{\Gamma\left(\frac{k}{2}+1\right)} x^{\frac{k}{2}} + O\left(x^{\frac{k}{2} - \frac{k}{k+1}}\right).$$

Aus dem bekannten Satze von Jacobi über die Anzahl der Darstellungen einer ganzen Zahl als Summe von vier Quadraten leitet Landau in der Fußnote [1]) unter IV genannten Abhandlung auf elementarem Wege das gegenüber (2) bessere Resultat

$$F_4(x) = \frac{\pi^2}{2} x^2 + O(x^{1+\varepsilon})$$

her. Eine analoge Verschärfung läßt sich auch für $k = 8$ erzielen, und zwar folgendermaßen.

Nach Jacobi ist für ganzes $n \geqq 1$

$$(3) \qquad \sum_{m_1^2 + \ldots + m_8^2 = 2n-1} 1 = 16 \sum_{m \mid (2n-1)} m^3,$$

$$(4) \qquad \sum_{m_1^2 + \ldots + m_8^2 = 2n} 1 = 16 \sum_{m \mid 2n} m^3 - 32 \sum_{(2m-1) \mid 2n} (2m-1)^3.$$

Wir haben ferner

$$\sum_{m \mid n \leqq x} m^3 = \sum_{mn \leqq x} m^3 = \sum_{n \leqq x} \sum_{m \leqq \frac{x}{n}} m^3$$

$$= \frac{1}{4} \sum_{n \leqq x} \left[\frac{x}{n}\right]^2 \left(\left[\frac{x}{n}\right] + 1\right)^2 = \frac{1}{4} \sum_{n \leqq x} \left(\frac{x^4}{n^4} + O\left(\frac{x^3}{n^3}\right)\right)$$

$$(5) \qquad = \frac{1}{4} \sum_{n=1}^{\infty} \frac{1}{n^4} x^4 + O(x^3),$$

und weiterhin

$$\sum_{(2m-1) \mid 2n \leqq x} (2m-1)^3 = \sum_{(2m-1) \mid n \leqq \frac{x}{2}} (2m-1)^3 = \sum_{m \mid n \leqq \frac{x}{2}} m^3 - \sum_{2m \mid n \leqq \frac{x}{2}} (2m)^3$$

$$= \sum_{m \mid n \leqq \frac{x}{2}} m^3 - 8 \sum_{2m \mid 2n \leqq \frac{x}{2}} m^3 = \sum_{m \mid n \leqq \frac{x}{2}} m^3 - 8 \sum_{m \mid n \leqq \frac{x}{4}} m^3$$

$$(6) \qquad = \frac{1}{128} \sum_{n=1}^{\infty} \frac{1}{n^4} x^4 + O(x^3).$$

Aus (3), (4), (5) und (6) folgt schließlich

$$F_8(x) = 1 + 16 \sum_{m \mid n \leqq x} m^3 - 32 \sum_{(2m-1) \mid 2n \leqq x} (2m-1)^3$$

$$= \frac{15}{4} \sum_{n=1}^{\infty} \frac{1}{n^4} x^4 + O(x^3),$$

d. h.

$$F_8(x) = \frac{\pi^4}{24} x^4 + O(x^3).$$

Ich will jetzt, allerdings gestützt auf ein neueres Resultat, für alle $k \geqq 5$

$$F_k(x) = \frac{\pi^{\frac{k}{2}}}{\Gamma\left(\frac{k}{2}+1\right)} x^{\frac{k}{2}} + O\left(x^{\frac{k}{2}-1}\right) \tag{7}$$

beweisen.

Nach G. H. Hardy[2]) ist für $k \geqq 5$

$$\sum_{m_1^2 + \ldots + m_k^2 = n} 1 = \frac{\pi^{\frac{k}{2}}}{\Gamma\left(\frac{k}{2}\right)} n^{\frac{k}{2}-1} \sum_{q=1}^{\infty} \sum_{p=0}^{q-1}{}' \left(\frac{S_{p,q}}{q}\right)^k e^{-\frac{2\pi i n p}{q}} + O\left(n^{\frac{k}{4}}\right). \tag{8}$$

Hierbei durchläuft p nur die zu q primen Werte, so daß $p = 0$ lediglich zu $q = 1$ gehört, während

$$S_{p,q} = \sum_{m=0}^{q-1} e^{\frac{2\pi i m^2 p}{q}}$$

ist. Die unendliche Reihe in (8) konvergiert wegen

$$|S_{p,q}| \leqq \sqrt{2q} \tag{9}$$

absolut. Ich sondere das Glied $q = 1$, $p = 0$ ab und summiere über $n \leqq x$. Das ergibt, zunächst für $k \geqq 8$,

$$F_k(x) = \frac{\pi^{\frac{k}{2}}}{\Gamma\left(\frac{k}{2}\right)} \sum_{n \leqq x} n^{\frac{k}{2}-1} + \frac{\pi^{\frac{k}{2}}}{\Gamma\left(\frac{k}{2}\right)} \sum_{q=2}^{\infty} \sum_{p=1}^{q-1}{}' \left(\frac{S_{p,q}}{q}\right)^k \sum_{n \leqq x} n^{\frac{k}{2}-1} e^{-\frac{2\pi i n p}{q}} + O\left(x^{\frac{k}{4}+1}\right)$$

$$= \frac{\pi^{\frac{k}{2}}}{\Gamma\left(\frac{k}{2}+1\right)} x^{\frac{k}{2}} + \frac{\pi^{\frac{k}{2}}}{\Gamma\left(\frac{k}{2}\right)} \sum_{q=2}^{\infty} \sum_{p=1}^{q-1}{}' + O\left(x^{\frac{k}{2}-1}\right). \tag{10}$$

[2]) G. H. Hardy, „On the representation of a number as the sum of any number of squares and in particular of five", Transactions of the American Mathematical Society **21** (1920), S. 255—284. Vgl. auch den Vorbericht, „On the expression of a number as the sum of any number of squares, and in particular of five or seven", Proceedings of the National Academy of Sciences **4** (1918), S. 189—193.

Der Leser kann übrigens (8) — aber ohne die Verschärfung für kleine k, von der sogleich die Rede sein wird, — auch als Spezialfall von (14) weiter unten kennen lernen.

Dies bleibt aber auch für $5 \leqq k \leqq 7$ gültig, da dann, wie Hardy a. a. O. nachgewiesen hat, das O-Glied in (8) identisch verschwindet.

Für $q \geqq 2$, $m \geqq 1$ ist

$$\left| \sum_{n=1}^{m} e^{-\frac{2\pi i n p}{q}} \right| < \operatorname{Max}\left(\frac{q}{p}, \frac{q}{q-p}\right) = r.$$

Somit liefert partielle Summation

$$\left| \sum_{n \leqq x} n^{\frac{k}{2}-1} e^{-\frac{2\pi i n p}{q}} \right| \leqq r \sum_{n \leqq x} \left((n+1)^{\frac{k}{2}-1} - n^{\frac{k}{2}-1}\right) + r(x+1)^{\frac{k}{2}-1}$$

$$\leqq 2r(x+1)^{\frac{k}{2}-1}. \tag{11}$$

Aus (9) und (11) folgt

$$\left| \sum_{q=2}^{\infty} \sum_{p=1}^{q-1}{}' \left(\frac{S_{p,q}}{q}\right)^k \sum_{n \leqq x} n^{\frac{k}{2}-1} e^{-\frac{2\pi i n p}{q}} \right| \leqq \sum_{q=2}^{\infty} \sum_{p=1}^{q-1}{}' \left|\frac{S_{p,q}}{q}\right|^k \left| \sum_{n \leqq x} n^{\frac{k}{2}-1} e^{-\frac{2\pi i n p}{q}} \right|$$

$$\leqq 2^{\frac{k}{2}+1} \sum_{q=2}^{\infty} \sum_{p=1}^{q-1}{}' \frac{r}{q^{\frac{k}{2}}} (x+1)^{\frac{k}{2}-1} \leqq 2^{\frac{k}{2}+2} \sum_{q=2}^{\infty} \frac{1+\log q}{q^{\frac{k}{2}-1}} (x+1)^{\frac{k}{2}-1} = O\left(x^{\frac{k}{2}-1}\right). \tag{12}$$

(10) und (12) ergeben schließlich (7).

Durch eine passende Verallgemeinerung von (8) mittels der Hardyschen Methode soll jetzt, unter der Voraussetzung rationaler $\alpha_{\mu\nu}$, $\alpha_1, \ldots, \alpha_k$, für alle $k \geqq 8$

$$\sum_{Q \leqq x} e^{2\pi i(\alpha_1 m_1 + \ldots + \alpha_k m_k)} = \delta \frac{\pi^{\frac{k}{2}}}{\sqrt{D}\, \Gamma\left(\frac{k}{2}+1\right)} x^{\frac{k}{2}} + O\left(x^{\frac{k}{2}-1}\right) \tag{13}$$

nachgewiesen werden; δ hat natürlich dieselbe Bedeutung wie in (1).

Beim Beweise dürfen die $\alpha_{\mu\nu}$ als ganz angenommen werden, da der allgemeine Fall auf diesen durch eine triviale Substitution zurückgeführt wird.

Es sei $H > 0$ der Hauptnenner von $\alpha_1, \ldots, \alpha_k$. Alle O-Zeichen sind in der Folge so zu interpretieren, daß die in ihnen implizite enthaltenen Konstanten lediglich von Q und H abhängen dürfen.

Die gewünschte Verallgemeinerung von (8) lautet

$$A(n) = \frac{\pi^{\frac{k}{2}}}{\sqrt{D}\, \Gamma\left(\frac{k}{2}\right)} n^{\frac{k}{2}-1} \sum_{\substack{q=1 \\ q \equiv 0 \,(\mathrm{mod}\, H)}}^{\infty} \sum_{p=0}^{q-1}{}' \frac{S_{p,q,(\alpha)}}{q^k} e^{-\frac{2\pi i n p}{q}} + O\left(n^{\frac{k}{4}}\right) \quad (k \geqq 5), \tag{14}$$

wobei (die Definition gilt für alle $-\infty < n < \infty$)

$$A(n) = \sum_{Q(m)=n} \exp\{2\pi i(\alpha_1 m_1 + \ldots + \alpha_k m_k)\}, \tag{15}$$

und ferner

$$S_{p,q,(\alpha)} = \sum_{(a)=0}^{q-1} \exp\left\{2\pi i \frac{p}{q} Q(a) + 2\pi i(\alpha_1 a_1 + \ldots + \alpha_k a_k)\right\}. \tag{16}$$ [3])

Für $\Re(s) > 0$ sei

$$\theta(s) = \theta(s, Q, (\alpha)) = \sum_{(m)=-\infty}^{\infty} \exp\{-\pi Q(m)s + 2\pi i(\alpha_1 m_1 + \ldots + \alpha_k m_k)\} \tag{17}$$

Wegen (15) wird dann zugleich

$$\theta(s) = \sum_{m=-\infty}^{\infty} A(m) e^{-m\pi s},$$

und hieraus

$$A(n) = e^{n\pi s} \int_0^1 \theta(s - 2ui) e^{-2\pi i n u} du.$$

Ich nehme von jetzt ab $n \geqq 1$ an und setze $s = \frac{1}{n}$. Dann kommt

$$A(n) = e^{\pi} \int_0^1 \theta\left(\frac{1}{n} - 2ui\right) e^{-2\pi i n u} du. \tag{18}$$

Auf das Intervall $(0, 1)$ lege ich alle zu $\sqrt{n}$ gehörigen Fareypunkte $\gamma = \frac{p}{q}$ und füge auch die zugehörigen Medianten $\frac{p+p'}{q+q'}$ hinzu. Jeder Punkt

$$\gamma = \frac{p}{q}, \quad 0 \leqq p \leqq q \leqq \sqrt{n}, \quad (p, q) = 1$$

bestimmt dann ein Intervall (γ), das von γ bis zu den beiden nächsten Medianten reicht; $\gamma = \frac{0}{1}$ und $\frac{1}{1}$ sind in diesem Sinne als *ein* Punkt aufzufassen.

Verschiebe ich (γ) so, daß γ in den Nullpunkt hereinfällt, so sei das entstehende Intervall (γ_0). Nach bekannten Sätzen über Fareyreihen ist dann

$$|u| \leqq \frac{2}{q\sqrt{n}} \text{ in } (\gamma_0); \quad |u| \geqq \frac{1}{2q\sqrt{n}} \text{ in der Komplementärmenge.} \tag{19}$$

Aus (18) folgt, wenn noch zur Abkürzung

$$w = \frac{1}{n} - 2ui; \quad \Re\left(\frac{1}{w}\right) = \frac{n}{1 + 4n^2u^2} = \varrho \tag{20}$$

(letzteres für spätere Zwecke) gesetzt wird,

[3]) Ich schreibe (α); (a); $Q(a)$; $Q(m)$ für $\alpha_1, \ldots, \alpha_k$; $a_1, \ldots, a_k$; $Q(a_1, \ldots, a_k)$; $Q(m_1, \ldots, m_k)$. Ebenso sind alle analogen Abkürzungen zu verstehen.

$$A(n) = e^{\pi} \sum_{\gamma} \int_{(\gamma_0)} \theta\left(\frac{1}{n} - 2ui\right) e^{-2\pi i n u}\, du$$

$$= e^{\pi} \sum_{\gamma} \int_{(\gamma_0)} \theta(w - 2\gamma i)\, e^{-2\pi i n (u+\gamma)}\, du. \tag{21}$$

Aus (17) folgt

$$\theta(w - 2\gamma i) = \sum_{(a)=0}^{q-1} \sum_{(b)=-\infty}^{\infty} \exp\{-\pi Q(a+bq)(w - 2\gamma i) + 2\pi i \sum_{\nu=1}^{k} \alpha_\nu (a_\nu + b_\nu q)\}$$

$$= \sum_{(a)=0}^{q-1} \exp\{2\pi i \gamma Q(a)\} \sum_{b=-\infty}^{\infty} \exp\{-\pi Q(a+bq) w + 2\pi i \sum_{\nu=1}^{k} \alpha_\nu (a_\nu + b_\nu q)\}$$

$$= D^{-\frac{1}{2}} q^{-k} w^{-\frac{k}{2}} \sum_{(b)=-\infty}^{\infty} \exp\left\{-\pi \bar{Q}(b - \alpha q) \frac{1}{q^2 w}\right\} \sum_{(a)=0}^{q-1} \exp\left\{2\pi i \gamma Q(a) + \frac{2\pi i}{q} \sum_{\nu=1}^{k} a_\nu b_\nu\right\}. \text{ [4]}$$

Hierbei ist $\Re(w^{-\frac{k}{2}}) > 0$ und $\bar{Q}$ die zu Q inverse Form.

Ich will jetzt

$$\sum_{(a)=0}^{q-1} \exp\left\{2\pi i \gamma Q(a) + \frac{2\pi i}{q} \sum_{\nu=1}^{k} a_\nu b_\nu\right\} = O(q^{\frac{k}{2}}) \tag{23}$$

nachweisen.

Es ist

$$\left|\sum_{(a)=0}^{q-1}\right|^2 = \sum_{(g),(h)=0}^{q-1} \exp\left\{2\pi i \gamma (Q(g) - Q(h)) + \frac{2qi}{q} \sum_{\nu=1}^{k} (g_\nu - h_\nu) b_\nu\right\}.$$

Werden neue Summationsbuchstaben (h), (l) durch $(g) = (h + l)$ eingeführt, so folgt

$$\left|\sum_{(a)=0}^{q-1}\right|^2 = \sum_{(l)=0}^{q-1} \exp\left\{2\pi i \gamma Q(l) + \frac{2\pi i}{q} \sum_{\nu=1}^{k} l_\nu b_\nu\right\} \sum_{(h)=0}^{q-1} \exp\left\{4\pi i \gamma \sum_{\mu,\nu=1}^{k} a_{\mu\nu} h_\mu l_\nu\right\}.$$

Die innere Summe ist nur dann von Null verschieden, und zwar $= q^k$, wenn

$$2\sum_{\nu=1}^{k} a_{1\nu} l_\nu \equiv 0, \ldots, \qquad 2\sum_{\nu=1}^{k} a_{k\nu} l_\nu \equiv 0 \pmod{q}.$$

Dieses System vor Kongruenzen, in Verbindung mit

$$0 \leqq (l) \leqq q - 1,$$

hat nur $O(1)$ Lösungen [5]. Daher ist in der Tat

$$\left|\sum_{(a)=0}^{q-1}\right|^2 = O(q^k).$$

---

[4] Vgl. A. Krazer, „Lehrbuch der Thetafunktionen", Leipzig: B. G. Teubner 1903, S. 108.

[5] Vgl. z. B. P. Bachmann, „Die Arithmetik der quadratischen Formen", Leipzig: B. G. Teubner 1898, S. 353.

Es werde zur Abkürzung

$$(24)\quad S(u)=D^{-\frac{1}{2}}q^{-k}w^{-\frac{k}{2}}\sum_{(b)=-\infty}^{\infty}{}'\exp\left\{-\pi\bar{Q}(b-\alpha q)\frac{1}{q^2w}\right\}\sum_{(a)=0}^{q-1}\exp\left\{2\pi i\gamma Q(a)+\frac{2\pi i}{q}\sum_{\nu=1}^{k}\right.$$

gesetzt. Hierbei ist für $q\not\equiv 0 \pmod H$ die volle Summe zu nehmen, andernfalls das Glied $(b-\alpha q)=0$ wegzulassen. Unser nächstes Ziel ist der Nachweis von

$$(25)\qquad \sum_{\gamma}\int_{(\gamma_0)} S(u)e^{-2\pi in(u+\gamma)}\,du=O(n^{\frac{k}{4}}).$$

Aus (20), (23) und (24) folgt zunächst

$$S(u)=O\left(q^{-\frac{k}{2}}|w|^{-\frac{k}{2}}\sum_{(b)=-\infty}^{\infty}{}'\exp\left\{-\pi\bar{Q}(b-\alpha q)\frac{\varrho}{q^2}\right\}\right)$$

und hieraus, mit einem nur von Q abhängigen $\tau>0$,

$$S(u)=O\left(q^{-\frac{k}{2}}|w|^{-\frac{k}{2}}\sum_{(b)=-\infty}^{\infty}{}'\exp\left\{-\frac{\varrho\tau}{q^2}\sum_{\nu=1}^{k}(b_\nu-\alpha_\nu q)^2\right\}\right)$$

$$=O\left(q^{-\frac{k}{2}}|w|^{-\frac{k}{2}}\sum_{(b)=0}^{\infty}\exp\left\{-\frac{\varrho\tau}{q^2}\left(b_1+\frac{1}{H}\right)^2-\frac{\varrho\tau}{q^2}\sum_{\nu=2}^{k}b_\nu^2\right\}\right).$$

Nach (19) und (20) ist

$$\frac{\varrho}{q^2}\geqq\frac{n}{q^2+16n}\geqq\frac{1}{17}.$$

Somit ergibt sich aus dem Vorigen

$$S(u)=O\left(q^{-\frac{k}{2}}|w|^{-\frac{k}{2}}\sum_{b_1=0}^{\infty}\exp\left\{-\frac{\varrho\tau}{q^2}\left(b_1+\frac{1}{H}\right)^2\right\}\right)$$

$$=O\left(q^{-\frac{k}{2}}|w|^{-\frac{k}{2}}\exp\left\{-\frac{\varrho\tau}{2H^2q^2}\right\}\right).$$

Wegen $\varrho=n^{-1}|w|^{-2}$ (vgl. (20)) ist weiter

$$S(u)=O\left(n^{\frac{k}{4}}(nq^2|w|^2)^{-\frac{k}{4}}\exp\left\{-\frac{\tau}{2H^2nq^2|w|^2}\right\}\right)=O\left(n^{\frac{k}{4}}\right).$$

Nach (19) ist daher

$$\int_{(\gamma_0)} S(u)e^{-2\pi in(u+\gamma)}\,du=O(n^{\frac{k}{4}-\frac{1}{2}}q^{-1}).$$

Zu jedem q gehören $\varphi(q)\leqq q$ Werte von p, d. h. es wird, wie behauptet,

$$\sum_{\gamma}\int_{(\gamma_0)} S(u)e^{-2\pi in(u+\gamma)}\,du=\Big(\sum_{q\leqq\sqrt{n}}n^{\frac{k}{2}-\frac{1}{2}}\Big)=O(n^{\frac{k}{4}}).$$

Aus (16), (21), (22), (24) und (25) folgt nunmehr

$$(26) \qquad A(n) = \frac{e^{\pi}}{\sqrt{D}} \sum_{\substack{q \leqq \sqrt{n} \\ q \equiv 0 \pmod H}} \sum_{p=0}^{q-1}{}' \frac{S_{p,q,(\alpha)}}{q^k} \int_{(\gamma_0)} w^{-\frac{k}{2}} e^{-2\pi i n \left(u + \frac{p}{q}\right)} du + O(n^{\frac{k}{4}}).$$

Da in (23) speziell

$$(23a) \qquad S_{p,q,(\alpha)} = O(q^{\frac{k}{2}})$$

enthalten ist, so ergibt sich wegen (19) und (20), falls in (26) jedes (γ_0) durch $-\infty < u < \infty$ ersetzt wird, ein Fehler von der Größenordnung

$$O\left(\sum_{q \leqq \sqrt{n}} q^{1-\frac{k}{2}} \int_{\frac{1}{2q\sqrt{n}}}^{\infty} \frac{du}{\left(\frac{1}{n^2} + 4u^2\right)^{\frac{k}{4}}} \right) = O(n^{\frac{k}{4}}).$$

Eine Anwendung des Cauchyschen Integralsatzes liefert ferner

$$\int_{-\infty}^{\infty} w^{-\frac{k}{2}} e^{-2\pi i n \left(u + \frac{p}{q}\right)} du = e^{-\pi} \frac{\pi^{\frac{k}{2}}}{\Gamma\left(\frac{k}{2}\right)} n^{\frac{k}{2}-1} e^{-\frac{2\pi i n p}{q}}.$$

Somit ergibt sich aus (26)

$$A(n) = \frac{\pi^{\frac{k}{2}}}{\sqrt{D}\,\Gamma\left(\frac{k}{2}\right)} n^{\frac{k}{2}-1} \sum_{\substack{q \leqq \sqrt{n} \\ q \equiv 0 \pmod H}} \sum_{p=0}^{q-1}{}' \frac{S_{p,q,(\alpha)}}{q^k} e^{-\frac{2\pi i n p}{q}} + O(n^{\frac{k}{4}}).$$

Um von hier aus zu (14) zu gelangen, hat man q über alle Werte $q \geqq 1$, $q \equiv 0 \pmod H$ laufen zu lassen. Der Fehler ist nach (23a) von erlaubter Größenordnung

$$O(n^{\frac{k}{2}-1} \sum_{q > \sqrt{n}} q^{1-\frac{k}{2}}) = O(n^{\frac{k}{4}}).$$

Aus (14) folgt jetzt (13) genau so, wie früher (7) aus (8). Für $H > 1$ fehlt in (14) das Glied $q = 1$, $p = 0$ und daran liegt es, daß in (13) $\delta = 0$ wird.

Wiesbaden, 7. Mai 1923.

(Eingegangen am 9. Juni 1923.)

Über die Erweiterung des Körpers der p-adischen Zahlen zu einem algebraisch abgeschlossenen Körper.

Von

Michael Bauer in Budapest.

1. Das Problem der Erweiterung eines Körpers zu einem algebraisch abgeschlossenen Körper wurde von H. Steinitz in seiner grundlegenden Abhandlung „Algebraische Theorie der Körper“ gelöst[1]). In derselben Abhandlung[2]) gab er auf Grund Henselscher Tatsachen eine spezielle Methode für den Körper $K(p)$ der rationalen p-adischen Zahlen. Die vorliegende Arbeit wird die letztgenannte Aufgabe auf solche Weise lösen, daß die Wurzeln der gewöhnlichen algebraischen Gleichungen im erweiterten Körper mit den gewöhnlichen Wurzeln als identisch betrachtet werden können[3]).

2. Wir betrachten den Körper der gewöhnlichen algebraischen Zahlen als gegeben. Aus diesem Körper soll eine Folge

$$\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots \tag{1}$$

mit den folgenden Eigenschaften ausgewählt werden. Jede algebraische Zahl ω soll in einem der Körper $K(\alpha_i)$ vorkommen. Der Körper $K(\alpha_{i+1})$ sei ein Galoisscher Körper, der den Körper $K(\alpha_i)$ enthält. Die rationale Primzahl p soll in den Körpern

$$K(\alpha_1), K(\alpha_2), \ldots, K(\alpha_n), \ldots \tag{1*}$$

[1]) Journal für Mathematik **137** (1910), S. 167—309.

[2]) A. a. O. S. 305.

[3]) Vgl. meine Arbeit „Die Theorie der p-adischen bzw. $\mathfrak{P}$-adischen Zahlen und die gewöhnlichen algebraischen Zahlkörper.“ Math. Zeitschrift **14** (1922), S. 244—249. Das im Texte gegebene Verfahren zur Bildung des erweiterten Körpers kann im gewissen Sinne als eine Verallgemeinerung der Henselschen Konstruktion der rationalen p-adischen Zahlen aus $K(1)$ gelten.

durch die Primideale

$$\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_n, \ldots \tag{2}$$

teilbar sein und $\mathfrak{P}_i$ sei ein Vielfaches von $\mathfrak{P}_{i+1}$. Jeder algebraischen Zahl ω wird durch die folgende Vorschrift eine Höhe in bezug auf p zugeordnet. Ist ω eine Größe von $K(\alpha_i)$, dann soll die Höhe

$$h = h(\omega) = \frac{a_i}{e_i} \tag{3}$$

ausfallen, wo a_i bzw. e_i die Ordnungen der Zahlen ω bzw. p in bezug auf $\mathfrak{P}_i$ sind[4]). Es ist evident, daß dieser Quotient derselbe bleibt, wenn man ω als Größe eines anderen Körpers (1*) betrachtet, infolgedessen ist die Höhe durch die Folge (2) eindeutig bestimmt. Die Bewertung von ω sei folgenderweise definiert: Für Null soll sie gleich Null sein, ist $\omega \neq 0$, so soll die Bewertung $|\omega| = e^{-h}$ ausfallen, wo $e > 1$ eine fix gegebene reelle Zahl ist. Die Bewertung eines Produkts ist gleich dem Produkte der Bewertungen der Faktoren. Die Bewertung einer Summe ist nicht größer als die Bewertungen der einzelnen Glieder und gleich der Bewertung des Gliedes, dessen Bewertung die größte ist, falls ein einziges solches Glied existiert. Es können die Fundamentalreihen eingeführt werden, die gewöhnlichen Gesetze bleiben bestehen[5]). Die Gesamtheit der Grenzwerte bildet einen Körper $\mathfrak{K}$, der eine perfekte Erweiterung von $K(p)$ ist. Die Gesamtheit der algebraischen Größen von $\mathfrak{K}$ soll durch $\bar{\mathfrak{K}}$ bezeichnet werden, $\bar{\mathfrak{K}}$ stellt eine kleinste Erweiterung von $K(p)$ zu einem algebraisch abgeschlossenen Körper dar. Der Körper $\bar{\mathfrak{K}}$ ist von $\mathfrak{K}$ verschieden, dies wurde zuerst von H. Kürschák vermutet und von H. Ostrowski bewiesen[6]).

3. Es muß also nur gezeigt werden, daß jede in $K(p)$ irreduzible Gleichung

$$F(x) = x^m + C_1 x^{m-1} + \ldots + C_m = 0(p) \tag{4}$$

im erweiterten Bereiche genau m Wurzeln besitzt. Es wird sich beim

[4]) In der Arbeit „Zur allgemeinen Theorie der algebraischen Größen", Journal für Mathematik **132** (1907), S. 21–32 habe ich sämtliche Quotienten $\frac{a_i}{e_i}$, welche in bezug auf p gebildet werden können, untersucht und dieselben als charakteristische Zahlen bezeichnet.

[5]) Ist eine Fundamentalreihe keine Nullreihe, so haben die Glieder von einem gewissen Index angefangen dieselbe Bewertung. Diese Bewertung soll auch dem Grenzwerte zufallen, die Bewertungen der Grenzwerte haben auch die im Texte angeführte Eigenschaft.

[6]) A. Ostrowski, Über einige Fragen der allgemeinen Körpertheorie. Journal für Mathematik **143** (1913), S. 225–284.

Beweise ergeben, daß die Höhe der Wurzeln, wie dies nach Ostrowski sein muß, die Kürschákschе Regel befolgt[7]), also gleich der Ordnung von C_m in bezug auf p dividiert durch m ist. Man kann sich auf den Fall von ganzen p-adischen Koeffizienten beschränken. Ist die Diskriminante von F, $D(F) \sim p^d$, so besitzt die Diskriminante $D(f)$ der Näherungsgleichung

$$f(x) = x^m + c_1 x^{m-1} + \ldots + c_m = 0 \tag{5}$$

dieselbe Ordnung in bezug auf p, wenn nur die gewöhnlichen rationalen ganzen Zahlen c_k die Relationen

$$c_k \equiv C_k \pmod{p^{d+\Delta}}, \quad \Delta > 0 \qquad (k = 1, 2, \ldots, m)$$

erfüllen. Wird Δ genügend groß gewählt, so ist nach H. Hensel[8]) $f(x)$ p-adisch irreduzibel. Sind daher die Zahlen $\omega^{(j)}$ $(j = 1, 2, \ldots, m)$ die Wurzeln der Gleichung (5), dann ist p in den Körpern $K(\omega^{(j)})$ eine Primidealpotenz,

$$p = \mathfrak{p}^{(j)e} \tag{6}$$

und die Höhen der Zahlen $\omega^{(j)}$ sind gleich der Ordnung von c_m in bezug auf p dividiert durch m.[9]) Die Gesamtheit der Zahlen $\omega^{(j)}$ bildet einen Galoisschen Körper, welcher in einem der Körper (1*) enthalten ist. Bezeichnen wir einen der fraglichen Körper durch $K(\alpha)$, das zugehörige Primideal (2) soll durch $\mathfrak{P}$ bezeichnet werden. Jedes $\mathfrak{p}^{(j)}$ ist durch $\mathfrak{P}$ teilbar, die konjugierten Zahlen $\pi^{(j)}$ der Körper $K(\omega^{(j)})$ sollen genau $\mathfrak{p}^{(j)}$ enthalten.

4. Zur Konstruktion der Wurzeln werden wir ein modifiziertes Henselsches Verfahren gebrauchen, welches gewisse Normalformen für die-

[7]) J. Kürschák, Über Limesbildung und allgemeine Körpertheorie. Journa für Mathematik **142** (1913), S. 211—253; A. Ostrowski, Über sogenannte perfekte Körper. Journal für Mathematik **147** (1917), S. 196.

[8]) Theorie der algebraischen Zahlen **1** (1908), S. 68. Schon die Wahl $\Delta = 1$ genügt.

[9]) Die Behauptungen lassen sich verschiedenartig begründen. Es sollen hier folgende drei Beweise angeführt werden. a) Beide Behauptungen folgen sofort aus der Fußnote [12]) meiner Arbeit [3]). b) Daß p eine Primidealpotenz ist, folgt ohne Anwendung der Theorie der $\mathfrak{P}$-adischen Zahlen aus meiner Arbeit „Zur Theorie der Fundamentalgleichung", Journal für Mathematik **149** (1919), S. 89—96. Betrachtet man die Norm $N(\omega^{(j)})$, so ergibt sich sofort die zweite Behauptung. c) Beide Behauptungen sind beweisbar, wenn man die Ausführungen meiner Arbeit „Über die Erweiterung eines algebraischen Zahlkörpers durch Henselsche Grenzwerte", Acta Litt. ac Sc. Regiae Univ. Hung. Francisco-Josephinae **1** (1923), S. 74—79 mit dem Satze von Hensel kombiniert, nach welchem sämtliche Koeffizienten eines irreduziblen p-adischen Polynoms $g(x) = x^m + p_1 x^{m-1} + \ldots + p_m(p)$ ganze p-adische Zahlen sind, wenn p_m ganz ausfällt.

selben liefern wird. Es ist sowohl $D(F)$ als $D(f) \sim p^d$, sie sollen im Körper $K(\omega^{(j)}, \mathfrak{p}^{(j)})$ genau $\pi^{(j)l}$ enthalten. Da

$$F(x) \equiv f(x) \pmod{p^{d+\Delta}}, \qquad \Delta > 0$$

ausfällt, wird $F(\omega^{(j)})$ genau $\pi^{(j)l+s}$, $s > 0$ enthalten. Wird $\Delta > d$ gewählt, was geschehen soll, so ist

$$s > l. \tag{7}$$

Aus der Relation

$$D(F) = A(x)\,F(x) + B(x)\,F'(x)(p), \tag{8}$$

in welcher die Koeffizienten ganze rationale p-adische Zahlen sind, folgt, daß die Zahl $F'(\omega^{(j)})$ im Körper $K(\omega^{(j)}, \mathfrak{p}^{(j)})$ genau $\pi^{(j)l_1}$, $l_1 \leqq l$ enthält. Man kann die ganze Zahl $\eta_1^{(j)}$ des Körpers $K(\omega^{(j)})$ in der Weise wählen, daß im Körper $K(\omega^{(j)}, \mathfrak{p}^{(j)})$

$$F(\omega^{(j)} + \pi^{(j)b_1}\eta_1^{(j)}) \equiv 0 \pmod{\pi^{(j)l+s+1}} \tag{9}$$

ausfällt. Es ist nämlich

$$F(\omega^{(j)} + \pi^{(j)b_1}\eta_1^{(j)}) = F(\omega^{(j)}) + \pi^{(j)b_1}\eta_1^{(j)}F'(\omega^{(j)}) + \pi^{(j)2b_1}\eta_1^{(j)2}\frac{F''(\omega^{(j)})}{2!} + \cdots,$$

setzen wir

$$b_1 + l_1 = l + s, \tag{10}$$

dann wird

$$b_1 \geqq s, \qquad 2b_1 \geqq 2s > s + l \tag{10*}$$

und $\eta_1^{(j)}$ kann als ganze Zahl des Körpers $K(\omega^{(j)})$ so ausgewählt werden, daß die Relation (9) erfüllt wird. Das Verfahren ist fortsetzbar, die Exponenten $b_1, b_2, \ldots, b_r$ und die ganzen Zahlen $\eta_1^{(j)}, \eta_2^{(j)}, \ldots, \eta_r^{(j)}$ der Körper $K(\omega^{(j)})$ können in der Weise bestimmt werden, daß im Körper $K(\omega^{(j)}, \mathfrak{p}^{(j)})$

$$F(\omega^{(j)} + \sum_{k=1}^{r}\pi^{(j)b_k}\eta_k^{(j)}) \equiv 0 \pmod{\pi^{(j)l+s+r}} \quad (j = 1, 2, \ldots, m) \tag{11}$$

ausfällt und noch die Relationen

$$b_k \geqq s + k - 1 \qquad (k = 1, 2, \ldots, r) \tag{11*}$$

gelten[10]). Die Wurzeln der Gleichung (4) werden durch die konvergenten Reihen

$$\eta^{(j)} = \omega^{(j)} + \sum_{k=1}^{\infty}\pi^{(j)b_k}\eta_k^{(j)} \qquad (j = 1, 2, \ldots, m) \tag{12}$$

[10]) Die Exponenten b_k bilden nicht notwendig eine monotone Folge.

geliefert, welche Größen des Körpers $K(\alpha, \mathfrak{P})$ darstellen[11]). Die Abschnitte der Reihen (12) mit gleicher Gliederanzahl sind konjugierte Zahlen der Körper $K(\omega^{(j)})$, sie bilden die Wurzeln von irreduziblen Gleichungen mit rationalen ganzen Koeffizienten, ihre Höhen sind gleich den Ordnungen der absoluten Glieder in bezug auf p dividiert durch m; infolgedessen sind die Höhen der Zahlen $\eta^{(j)}$ gleich der Ordnung von C_m in bezug auf p, dividiert durch m, was zu beweisen war.

Es ist noch zu ersehen, daß man bei einer anderen Wahl der Folgen (1) und (2) vom Körper $\mathfrak{K}$ zu einem isomorphen Körper übergeht.

[11]) Die Größen $\eta^{(j)}$ sind verschieden. Es ist nämlich: $\eta^{(j)} \equiv \omega^{(j)} \pmod{\pi^{(j)l+1}}$, woraus die Behauptung folgt, weil im entgegengesetzten Falle $D(F) \equiv 0 \pmod{p^{d+1}}$ wäre.

(Eingegangen am 26. Juni 1923.)

Zum Vertrieb wurde mir übergeben:

Carl Friedrich Gauss Werke

Herausgegeben von der

Gesellschaft der Wissenschaften zu Göttingen

Band I. **Disquisitiones arithmeticae.** Zweiter Abdruck. 478 S. gr. 4°. 1870.
Geb. 48 Goldmark / 15,60 Dollar

„ II. **Höhere Arithmetik.** Zweiter Abdruck. 528 S. gr. 4°. 1876.
Geb. 53 Goldmark / 17,20 Dollar

Nachtrag zum ersten Abdruck des II. Bandes. 33 S. gr. 4°. 1876.
Geb. 3,80 Goldmark / 1,20 Dollar

„ III. **Analysis.** Zweiter Abdruck. 499 S. gr. 4°. 1876. Geb. 50 Goldmark / 16,25 Dollar

„ IV. **Wahrscheinlichkeitsrechnung und Geometrie.** Zweiter Abdruck. 492 S. gr. 4°. 1880.
Geb. 50 Goldmark / 16,25 Dollar

„ V. **Mathematische Physik.** Zweiter Abdruck. 642 S. gr. 4°. 1877.
Geb. 64 Goldmark / 21 Dollar

„ VI. **Astronomische Abhandlungen und Aufsätze.** 664 S. gr. 4°. 1874.
Geb. 69 Goldmark / 22,40 Dollar

„ VII. **Theoretische Astronomie.** 650 S. gr. 4°. 1906. Geb. 65 Goldmark / 21,20 Dollar

„ VIII. **Arithmetik, Analysis, Wahrscheinlichkeitsrechnung, Geometrie.** (Nachträge zu Band I—IV.) 458 S. gr. 4°. 1900. Geb. 46 Goldmark / 15 Dollar

„ IX. **Geodäsie.** (Fortsetzung von Band IV.) 528 S. gr. 4°. 1903. Geb. 53 Goldmark / 17,20 Dollar

„ X. Abteilung 1. **Nachlaß und Briefwechsel zur reinen Mathematik.** (Nachträge zu Band I bis IV und VIII. 586 S. und einer photographischen Nachbildung des Tagebuches. gr. 4°. 1917. Geb. 59 Goldmark / 19,20 Dollar

„ X. Abteilung 2. Abhandlung I und V. **Über Gauss' zahlentheoretische Arbeiten** von Paul Bachmann. — **Gauss und die Variationsrechnung** von Oscar Bolza. 74 und 95 S. gr. 4°. 1922. 17 Goldmark / 5,50 Dollar

„ X. Abteilung 2. Abhandlung IV. **Gauss als Geometer** von Paul Stäckel. 123 S. gr. 4°. 1923. 12,50 Goldmark / 4 Dollar

Weitere Bände befinden sich in Vorbereitung.

Nachbildung des Tagebuchs (Notizenjournals) 1796 bis 1814. 1,20 Goldmark / 0,40 Dollar

Materialien für eine wissenschaftliche

Biographie von Gauss

Gesammelt von

F. Klein, M. Brendel und L. Schlesinger

Heft 1. **Über Gauss' zahlentheoretische Arbeiten.** Von P. Bachmann in Weimar. III, 54 S. gr. 8°. 1911. 2,80 Goldmark / 1 Dollar

„ 2/3. C. F. Gauss: **Fragmente zur Theorie des arithmetisch-geometrischen Mittels aus den Jahren 1797 bis 1799. — Über Gauss' Arbeiten zur Funktionentheorie.** Von L. Schlesinger in Gießen. IV, 34 und 143 S. gr. 8°. 1912. 9 Goldmark / 2,90 Dollar

„ 4/5. **C. F. Gauss als Zahlenrechner.** Von A. Galle in Potsdam. — **C. F. Gauss als Geometer.** Von P. Stäckel in Heidelberg. IV, 142 S. gr. 8°. 1918. 7,20 Goldmark / 2,40 Dollar

„ 6. **Die Wechselwirkung zwischen Zahlenrechnen und Zahlentheorie bei C. F. Gauss.** Von Ph. Maennchen in Gießen. (IV, 47 S. gr. 8°. 1918. 2,40 Goldmark / 0,85 Dollar

„ 7. **Über die astronomischen Arbeiten von Gauss.** Von M. Brendel in Frankfurt a. M. Erster Abschnitt: Theoretische Astronomie. IV, 106 S. gr. 8°. 1919. 5,60 Goldmark / 1,80 Dollar

„ 8. **Zahlbegriff und Algebra bei Gauss.** Von A. Fraenkel in Marburg a. d. Lahn. Mit einem Anhang von A. Ostrowski in Göttingen: **Zum ersten und vierten Gauss'schen Beweise des Fundamentalsatzes der Algebra.** II, 59 S. gr. 8°. 1920. 3 Goldmark / 1 Dollar

Verlag von Julius Springer in Berlin W 9

Bei der Redaktion eingegangene Schriften.

Unter dieser Rubrik werden wir fortlaufend ein Verzeichnis derjenigen Schriften veröffentlichen, die uns von Verlegern oder Verfassern zu diesem Zwecke übersandt werden. Wir bitten, von dieser Gelegenheit zur Bekanntmachung neuer Schriften ausgiebig Gebrauch machen zu wollen.

v. Laue, Prof. Dr. M. **Die Relativitätstheorie.** 2. Band: Die allgemeine Relativitätstheorie und Einsteins Lehre von der Schwerkraft. 2. Auflage. Braunschweig, Fr. Vieweg & Sohn, 1921. (XII u. 276 S.)

Bohr, Prof. Dr. Niels. **Drei Vorträge über Spektren und Atombau.** Braunschweig, Fr. Vieweg & Sohn, 1922. (VI u. 148 S.)

Study, Prof. Dr. E. **Denken und Darstellung, Logik und Werte, Dingliches und Menschliches in Mathematik und Naturwissenschaften.** Braunschweig, Fr. Vieweg & Sohn, 1921. (IV u. 43 S.)

Kneser, Prof. Dr. A. **Die Integralgleichungen und ihre Anwendungen in der mathematischen Physik.** 2. Auflage. Braunschweig, Fr. Vieweg & Sohn, 1922. (VIII u. 292 S.)

Einstein, Prof. Dr. A. **Vier Vorlesungen über Relativitätstheorie,** gehalten im Mai 1921 an der Universität Princeton. Braunschweig, Fr. Vieweg & Sohn, 1822. (70 S.)

Study, Prof. Dr. E. **Mathematik und Physik.** Braunschweig, Fr. Vieweg & Sohn, 1923. (31 S.)

Seeliger, Prof. Dr. R. **Aufgaben aus der theoretischen Physik.** Braunschweig, Fr. Vieweg & Sohn, 1921. (X u. 154 S.)

Schlömilch, O., Kompendium der höheren Analysis. In sechster Auflage bearbeitet von **A. Kneser.** Erster Band. Braunschweig, Fr. Vieweg & Sohn, 1923. (X u. 620 S.)

Journal für die reine und angewandte Mathematik, Band 153, Heft 1/2, ausgegeben am 27. August, Berlin und Leipzig, Walter de Gruyter & Co. S. 1—140. 4°. 1923.

Jahrbuch über die Fortschritte der Mathematik, herausgegeben von L. Lichtenstein. Band 46, Jahrgang 1916—1918. Heft 2, S. 561—960. Vierter und fünfter Abschnitt (Analysis und Geometrie). Berlin und Leipzig, Walter de Gruyter & Co., 1923.

Nenning, A., Kosmische Dynamik. München-Zürich, Johannes Albert Mahr, 1923. (64 S.)

Druck von Oscar Brandstetter in Leipzig.